INTELLIGENCE INFO

ISSN 2821 - 8159, ISSN – L 2821 – 8159, Volumul 1, Numărul 1, Septembrie 2022

The impact of DoS (Denial of Service) cyberattacks on a Local Area Network (LAN)

Darius-Antoniu Ferenț

Pentru a cita acest articol: Ferenț, Darius-Antoniu (2022), The impact of DoS (Denial of Service) cyberattacks on a Local Area Network (LAN), *Intelligence Info*, **1**:1, 124-129, DOI: 10.58679/II52272, https://www.intelligenceinfo.org/the-impact-of-dos-denial-of-service-cyberattacks-on-a-local-area-network-lan/

Publicat online: 10.08.2022

The impact of DoS (Denial of Service) cyberattacks on a Local Area Network (LAN)

Darius-Antoniu Ferenț

Abstract

In this paper I will highlight a *modus operandi* of hackers launching Denial of Service (DoS) cyberattacks. I will theoretically show how CAM Overflow and TCP SYN Flood attacks can be performed, using Kali Linux, a Linux distribution used by cyber criminals to launch MitM (Man-in-the-Middle) attacks, DoS attacks, observing traffic in a computer network, etc. Hackers can affect the functioning of devices on an organization's local network (server, router, switch, etc.) by sending thousands of packets per second to the target device. CAM Overflow is an attack where a hacker aims to overcrowd the CAM table of a switch with MAC addresses, and TCP SYN Flood is an attack that can be launched against a server in the computer network.

Keywords: cyberattack, Denial of service (DoS), botnet, Local Area Network (LAN), cyber criminals, CAM Overflow.

Rezumat

În cadrul acestui articol voi evidenția un *modus operandi* al hackerilor care lansează atacuri cibernetice de tip Denial of Service (DoS). Voi arăta teoretic cum pot fi realizate atacurile CAM Overflow și TCP SYN Flood, utilizând Kali Linux, o distribuție de Linux utilizată de criminalii cibernetici pentru a putea lansa atacuri de tip MitM (Man-in-the-Middle), atacuri DoS, observarea traficului dintr-o rețea de calculatoare etc. Hackerii pot afecta funcționarea dispozitivelor din rețeaua locală a unei organizații (server, router, switch etc.) prin trimiterea a mii de pachete/secundă către dispozitivul țintă. CAM Overflow este un atac prin care un hacker urmărește să supra-aglomereze tabela CAM a unui switch cu adrese MAC, iar TCP SYN Flood este un atac care poate fi lansat împotriva unui server din rețeaua de calculatoare.

Cuvinte cheie: atac cibernetic, Denial of service (DoS), botnet, Local Area Network (LAN), criminali cibernetici, CAM Overflow.

INTELLIGENCE INFO, Volumul 1, Numărul 1, Septembrie 2022, pp. 124-129
ISSN 2821 - 8159, ISSN – L 2821 – 8159, DOI: 10.58679/II52272
URL: https://www.intelligenceinfo.org/the-impact-of-dos-denial-of-service-cyberattacks-on-a-local-area-network-lan/

A network is a collection of interconnected devices (computers, routers, switches, etc.) that exchange information via protocols. Network equipment such as switches, routers, servers, access points and modems play an important role in the networks' operation.

The size of a network can be determined by the number of computers integrated within the network, as well as by the geographical extent of the network. Networks are therefore divided into: Local area networks (known as LAN), Metropolitan area networks (MAN), Wide area networks (WAN). A LAN is a private network inside a building. A LAN works in people's homes, schools, offices, factories. A university campus network is also a LAN. Within a company or business, a larger LAN can be created by connecting switches together. A large LAN network can be organised into two smaller local area networks which leads to efficiency because such a network is easier to manage.

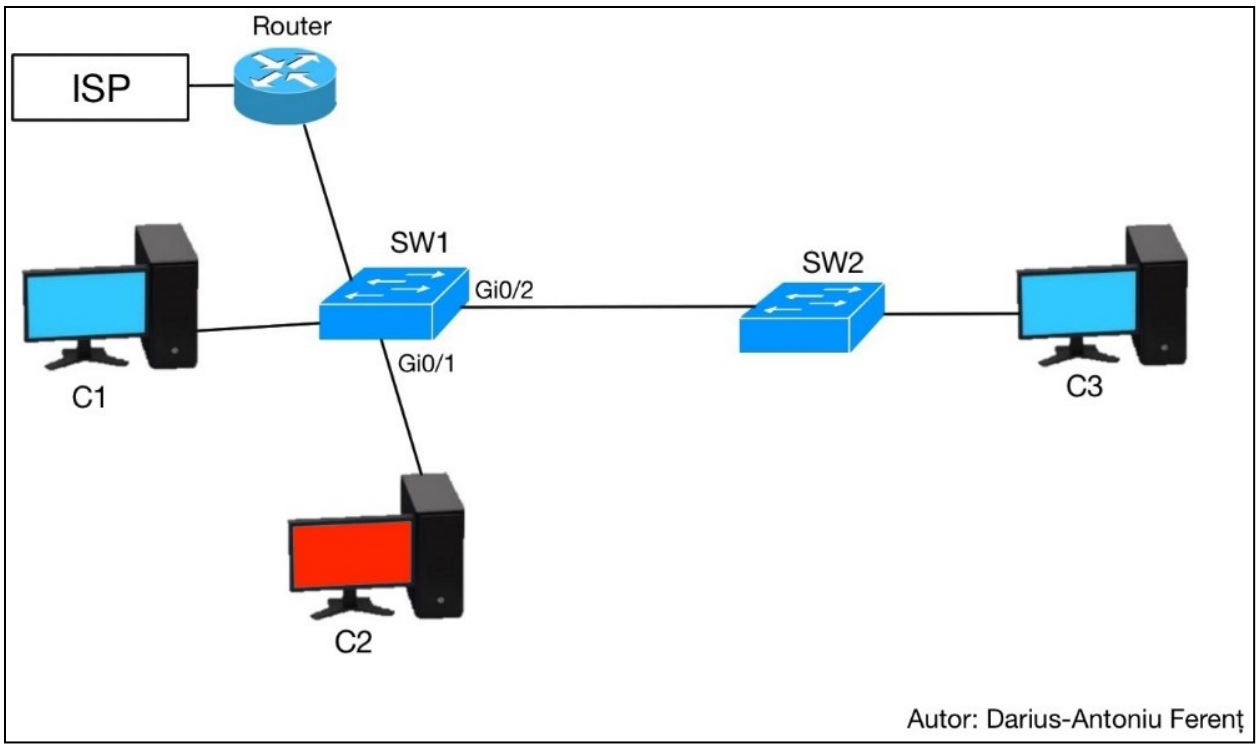
Wide area networks cover the area of a country or a continent. The Internet is considered a wide area network (planetary network), "consecrated by the phrase network of networks" (Pătrașcu 2018, p.24). The Internet is used globally and is particularly important in all sectors of human life. A wide area network is used to connect smaller, LAN-like networks so that computer users in location A can communicate with users and computers in location B.

> "Denial of Service (DoS) is a cyberattack aimed at blocking and making the resources of an IT&C system or network unavailable, by flooding the victim's system with an overwhelming amount of traffic or service requests to overload the web server, computer or network." (Ferenț 2022, p.43).

In order to emphasize the hackers' *modus operandi*, we will show how two Denial of Service (DoS) cyberattacks can theoretically be carried out and the impact they have on an IT&C system. To perform the CAM Overflow and TCP SYN Flood attacks we will use Kali Linux, a Linux distribution used by Black-Hat Hackers and White-Hat Hackers. The tools in Kali Linux are grouped into 14 categories, depending on what action or cyberattack a hacker wants to initiate. For example, Kali Linux has tools for scanning vulnerabilities in a computer network (Nmap, Nessus). A wide range of cyberattacks can also be launched using the Kali Linux toolkit: MitM attacks, Spoofing, DoS, web attacks, password cracking attacks, network traffic observation, etc.

CAM Overflow is a Denial of Service cyberattack that targets the overpopulation of a switch's CAM table. A switch is a network device that connects multiple devices (laptops, computers, servers) in a local area network (LAN). A switch sends data from one computing device to another based on the source and destination MAC addresses. Based on the source MAC address,

a switch remembers the port a device is on, and based on the destination MAC address, the switch sends traffic to a port. This information is stored by the switch in the CAM (Content Addressable Memory) table, which is limited. Depending on the model, a switch may hold several thousand MAC addresses. In order to illustrate a CAM Overflow cyberattack, we will design a local network in which we have two switches (SW1 and SW2), a router and three computers (C1, C2 and C3).



In our example, the hacker controls computer C2. Taking advantage of the fact that SW1 will learn the source MAC address on port Gi0/1, the hacker will send thousands of random source MACs per second from the C2 computing device, using Kali Linux. At that time, SW1 will retain all the source MACs received in the CAM table. If the CAM table fills up, SW1 will not retain any more MAC addresses. Note that the switch will not get blocked. When computer C1 wants to send information to computer C3, the switch will not know on which port to send that information, because other MAC addresses have appeared in the CAM table, so it will send traffic to all ports available to it (including computer C2 which is controlled by the attacker). For example, if the user at C1 is communicating with the user at computer C3 and there is an unencrypted connection between the two devices, when the switch sends the traffic to C2, the attacker can use the Wireshark tool in Kali Linux to listen for that traffic.

To avoid CAM Overflow attacks, it is recommended to use a set of port rules (Port Security). The solution is to limit the number of MAC addresses that can be learned on a port. If we observe that the C2 device sends a lot of MAC addresses in a short time, we set a limit. For example, on port Gi0/1 a maximum of two MAC addresses can be accessed simultaneously. If the C2 device sends more MAC addresses than the set limit, the Gi0/1 port will shut down.

For example, a malicious person in an institution wants to disconnect computer C2 and connect a new switch (SW3) to the network and three laptops to its ports. In this case, Port Security ensures that if more than two MAC addresses are sent on Gi0/1, that port shuts down.

Denial of Service (DoS) cyberattacks can also be launched using Metasploit, a complex tool in Kali Linux. By sending a very large number of packets in a very short time, cyber criminals can disrupt the operation of a server (e.g. mail server), router or computer equipment in the computer network of a firm, company or institution. The attacker can use the Metasploit tool to launch a TCP SYN Flood attack on a server in the network.

The TCP SYN cyberattack can be carried out due to the exchange of messages at the beginning of the Transmission Control Protocol (TCP). When a client sends a request (SYN) to a server, announcing its intention to start a conversation, the server designates an entry in the table of half-open connections and sends back an acceptance message (SYN-ACK), announcing its readiness. The client must respond with an ACK packet in order to start the communication. An attacker might never send this acknowledgement, causing the connection table to fill up, further legitimate requests thus being blocked (Nicolăescu 2011, p.29). In short, the hacker initiates many TCP connections to a server without completing the normal message exchange.

The users of computing devices (computer, laptop, smartphone, tablet, etc.) who do not use a firewall program and do not regularly update their anti-virus/anti-malware software, put their own computing equipment at risk of being infected with malware and integrated into a botnet, with which the hacker can launch DDoS (Distributed Denial of Services) attacks. Also, to prevent their computing devices from being infected with malware, users should fix security holes and software bugs in their operating systems by automatically or manually applying available updates.

After infecting hundreds or thousands of IT&C devices, a hacker can launch a DDoS attack to disrupt an entire network. These attacks are not easy to counteract, as a botnet can contain computers/devices distributed in different parts of the world (Ferenț 2022, p.44). The use of a firewall is very important for a firm, institution or a company because, by filtering traffic and

checking whether a downloaded file is safe or malicious, it may prevent DoS attacks, and turning network computers into zombies. A computer/laptop that has not been compromised by a malware infection cannot be turned into a bot. If the firewall notices a very large number of packets coming from a particular source, it will defensively remove them all. However, if the hacker uses the spoofing technique, the firewall is put in difficulty, as it cannot differentiate secure (legitimate) packets from malicious ones, coming from the same sources (Budiu 2001). At the same time, smartphones and tablets can be used to send spam emails or launch DDoS attacks, as these devices connect into the so-called zombie networks (Goodman 2016, p.201).

Bibliography

Budiu, Mihai (2001). „Atacuri distribuite în Internet" [*Shared attacks on the Internet*], available at: https://www.cs.cmu.edu/~mihaib/articole/ddos/ddos-html.html.

Ferenț, Darius-Antoniu (2022). *Ghid de securitate cibernetică [Cybersecurity guide]*, Cluj-Napoca, Casa Cărții de Știință Publishing House.

Goodman, Marc (2016). *X-Cyber: viitorul începe azi [The future starts today],* Bucharest, Rao Publishing House.

Nicolăescu, Nicu-Sebastian (2011). *Teză de doctorat: Contribuții privind monitorizarea securității rețelelor de calculatoare [PhD Thesis: Contributions on network security monitoring],* Bucharest, The Technical Military Academy.

Tanenbaum, Andrew, Wetherall, David (2011). *Computer Networks, 5th edition,* Pretince Hall Publishing House.

Pătrașcu, Petrișor (2018). „Infrastructurile cibernetice specifice sectorului tehnologiei informației" [*Cyber infrastructures specific to the IT sector*], *Buletinul Universității Naționale de Apărare Carol I [Bulletin of Carol I National Defense University],* available at: https://revista.unap.ro/index.php//revista/article/view/428/418.