**Denial of Service**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Target** | **Aspect** | **Type** | **How?** | **Attacker goal** | **example** |
| Network | devices |  | Config destruction/altering  Physical destruction | Intercept connection  Intercept connection | 15  27 |
| Link  Software /  Application |  | Protocol Attacks  Bandwidth/Throughput Attacks | Destruct communication mechanism  Block network link  Crash Network Software | 1, 2,21  3,5,6  4, 7,13, 22 |
| Server | Physical resources |  | Destruction of physical resources | Sabotage Server | 17 |
| Application/  software |  | Application Crashing  Data Destruction  Resource Depletion  exploiting security features | functionality Sabotage  delete records from Database/make data inaccessicble  memory/cpu/ram  exhaustion  Make service inaccessible | 19, 23,24,25,26  8,18  10,11  14 |
| Client | Physical  resourced |  | Physical destruction | Sabotage user machine | 28 |
| Application/  software |  | Application Crashing  Data Destruction  Resource Depletion | User Functionality sabotage  Remove user data/  Make data inaccessible  memory/cpu/ram  exhaustion | 16  8  12,24 |

**Concrete Examples**

1. **Smurf.** The attacker sends a large number of ICMP echo requests to a broadcast address. All the ICMP messages have spoofed source address as that victim’s IP address. Eventually all the reply messages target and flood the victim’s address [1]
2. **Fraggle.** A variation to the Smurf attack is the Fraggle attack. The attack is essentially the same as the Smurf attack but instead of sending an ICMP echo request to the direct broadcast address, it sends UDP packets. [2]
3. **Ping flood.** Ping flood is similar to Smurf wherein the victim is bombarded with thousands of ping packets. [1]
4. **Ping of death.** Ping of death is similar to Ping of death wherein the victim is sent corrupt packets that could crash the system. [1]
5. **TCP SYN Flood.** The above described methods works on consuming the bandwidth space whereas this attack aims at exploiting server CPU memory. Whenever a host attempts to connect to a server, a three-way handshake protocol is established before any actual data transfer occurs. Firstly, the host sends a SYN packet to initiate the handshake. The server then replies with an Acknowledgement packet. At last the host again needs to send a SYN ACK packet to establish a successful connection. But attackers leave the handshake half open by not sending the last SYN and the server keeps waiting for the host to send the final packet. When thousands of such half open connections are initiated, the server runs out of memory and crashes. It will not be able to serve the legitimate clients as its memory is dumped with forged fake packets. [1]
6. **UDP flood.** UDP flooding is similar to ping flood. Here instead of ping packets, UDP packets are bombarded against the server. UDP could be a lot more effective than ICMP in smaller networks as the size of the UDP packets are enormous. The packet size could be set up to 65000 bytes which could easily flood a given Ethernet network when multiple zombies are set up. This project has analyzed all the above described attacks and has brought down some interesting observations. [1]
7. **Land attack.** The attacker sends a spoofed TCP packet to the victim machine where the values of source and destination IP addresses are the same. When the victim machine receives such a packet, it communicates to itself continuously until the machine crashes. [3]
8. **Ransomware.** Ransomware is a type of malicious software that infects and restricts access to a computer until a ransom is paid. Although there are other methods of delivery, ransomware is frequently delivered through phishing emails and exploits unpatched vulnerabilities in software. [4]
9. **UDP port denial of service.** When a connection is established between two UDP services, each of which produces output, these two services can produce a very high number of packets that can lead to a denial of service on the machine(s) where the services are offered. Anyone with network connectivity can launch an attack; no account access is needed. For example, by connecting a host's chargen service to the echo service on the same or another machine, all affected machines may be effectively taken out of service because of the excessively high number of packets produced. In addition, if two or more hosts are so connected, the intervening network may also become congested and deny service to all hosts whose traffic traverses that network. [5] --- (identical to UDP flood)
10. **Email bombing/spamming.** Email bombing is characterized by abusers repeatedly sending an email message to a particular address at a specific victim site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial of service impact. Email spamming is a variant of bombing; it refers to sending email to hundreds or thousands of users (or to lists that expand to that many users). Email spamming can be made worse if recipients reply to the email, causing all the original addressees to receive the reply. It may also occur innocently, as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users, or as a result of a responder message (such as vacation(1)) that is setup incorrectly. Email bombing/spamming may be combined with email spoofing (which alters the identity of the account sending the email), making it more difficult to determine who actually sent the email. [6]
11. **Anonymous ftp config.** Denial of service by consuming the disk. [7]
12. **Intentional error generation.** Intentionally generating errors. The error must be logged and consume disk space[7]
13. **Denial of service attack via ping.** Use of ping command to construct oversized ICMP datagrams (which are encapsulated in IP packet) [8]
14. **Multiple login attempt.** Intruder attempt to login to a web with user account to lock user.
15. **Routing Configuration altering.** Intruder changes routing info in the routers making network inaccessible.
16. **Windows Registry altering.** Intruder modifies the registry information on windows registry making certain functions unavailable.
17. **Overheating server**
18. **SQL Injection/DELETE.** Using SQL Injection to make data inaccessible.
19. **Dll spoofing/Dos:** Using dll spoofing to make original dll inaccessible.
20. Malware (find specific name)
21. **DNS name server Attack:** his is one of the most common method for attacks, mainly by sending a high number of UDP based DNS requests to a nameserver using a spoof IP address, now any nameserver response is sent back to the destination i.e., to the spoofed IP address and here this IP address is the victim of the DoS attack. So, it is difficult for a nameserver or the victim to determine the true source of the attack.[10]
22. **Teardrop attack.** In this type of attack first a packet of small size is sent. Then another packet said to be the part of the first packet sent. The second packet sent is very small to pick it from the first packet, this causes an error is assembling and the system may crash or hang. Generally fragmentation is very necessary if the message size is large , at the receiving end all the fragmented packets are reassembled to complete it, teardrop attacks concentrate here and sends unrelated fragment packets, which leads to system crash or hang when trying to assemble them.
23. **XDOS** An XML denial-of-service attack (XDoS attack) is a content-borne denial-of-service attack whose purpose is to shut down a web service or system running that service. A common XDoS attack occurs when an XML message is sent with a multitude of digital signatures and a naive parser would look at each signature and use all the CPU cycles, eating up all resources. These are less common than inadvertent XDoS attacks which occur when a programming error by a trusted customer causes a handshake to go into an infinite loop.
24. **Buffer overrun**
25. **Malformed data.** Causing parser exception
26. **SQL Injection/shut down**
27. **Using USB-killer** to destroy router
28. **Using USB-killer** to destroy laptop

**Reference**

**[1]** [**https://www.sans.org/reading-room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi-33764**](https://www.sans.org/reading-room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi-33764)

**[2]** [**https://usa.kaspersky.com/resource-center/definitions/smurf-attack**](https://usa.kaspersky.com/resource-center/definitions/smurf-attack)

**[3]** [**http://insecure.org/sploits/land.ip.DOS.html**](http://insecure.org/sploits/land.ip.DOS.html)

**[4]** [**https://www.us-cert.gov/security-publications/Ransomware**](https://www.us-cert.gov/security-publications/Ransomware)

**[5]** [**https://www.cert.org/historical/advisories/CA-1996-01.cfm**](https://www.cert.org/historical/advisories/CA-1996-01.cfm)**?**

**[6]** [**https://www.cert.org/historical/tech\_tips/email\_bombing\_spamming.cfm**](https://www.cert.org/historical/tech_tips/email_bombing_spamming.cfm)**?**

**[7]** [**https://www.cert.org/information-for/denial\_of\_service.cfm**](https://www.cert.org/information-for/denial_of_service.cfm)

**[8]** [**http://www.securityfocus.com/advisories/968**](http://www.securityfocus.com/advisories/968)

**[9]** [**https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/**](https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/) **(referenced by cert)**

**[10]** <https://www.hostdepartment.com/blog/2014/05/21/ddos-attack/>

[11] <https://www.owasp.org/images/d/da/OWASP_IL_7_Application_DOS.pdf>