

Forum:[Hack Forums](#)

Thread: [\[TOOL\] ZARP - Network Attack Tool \[*nix\]](#)

Armada - December 17, 2015, 4:51 pm

ZARP - Network Attack Tool

Open Source/GitHub

Zarp is a network attack tool centered around the exploitation of local networks. This does not include system exploitation, but rather abusing networking protocols and stacks to take over, infiltrate, and knock out. Sessions can be managed to quickly poison and sniff multiple systems at once, dumping sensitive information automatically or to the attacker directly. Various sniffers are included to automatically parse usernames and passwords from various protocols, as well as view HTTP traffic and more. DoS attacks are included to knock out various systems and applications. These tools open up the possibility for very complex attack scenarios on live networks quickly, cleanly, and quietly.

The long-term goal of zarp is to become the master command center of a network; to provide a modular, well-defined framework that provides a powerful overview and in-depth analysis of an entire network. This will come to light with the future inclusion of a web application front-end, which acts as the television screen, whereas the CLI interface will be the remote. This will provide network topology reports, host relationships, and more. zarp aims to be your window into the potential exploitability of a network and its hosts, not an exploitation platform itself; it is the manipulation of relationships and trust felt within local intranets. Look for zeb, the web-app frontend to zarp, sometime in the future.

Features

zarp has around 30+ modules grouped into categories of attack and has multiple functionalities under each group:

- Poisoners
- Denial of Service
- Sniffers
- Scanners
- Services
- Parameter
- Attacks

[Direct Download](#)

[OG Site](#)

?

