# Shrew Attack

Arash Taherkalateh 882980

در کل حملات DoS را می‌توان به دو دسته تقسیم بندی کرد : High-rate و . Low-rate Shrew Attack از دسته حملات Low-rate است. این دسته از حملات هرچند کمتر شناخته شده و استفاده شده هستند، با این حال نه تنها میتوانند به اندازه حملات High-rate مخرب، که بعضا خطرناک‌تر هم باشند، چرا که در اینجا تشخیص حمله از طریق ترافیک روی Router و یا DoS Counter سخت‌تر صورت می‌پذیرد.

Shrew Attack در دسته حملات Low-rate قرار دارد . این حمله از ضعف‌های موجود در الگوریتم TCP برای به هم ریختن ارتباط استفاده می‌کند . در کل TCP و الگوریتم کنترل تراکم در آن ( TCP's Congestion Control ) مطمئن و پایدار است. با این حال برخی مفروضات درباره همکاری End-System در اینجا ممکن است راه را برای Attacker باز بگذرد .

اما این حمله چگونه کار می‌کند ؟ Shrew Attack تشکیل شده است از ارسال تعدادی بسته TCP با فواصل زمانی مشخص . این بسته‌ها با بسامدی کم و مشخص و در عین حال زمان‌بندی مشخص ترافیکی ایجاد میکنند که میتواند از مکانیزم Time-out خوردن ( Retransmission Time out mechanism ) و ارسال مجدد بسته‌ها سوأستفاده کند . تکرار این الگو در نهایت قادر است گلوگاه ارتباطی را تنگ کرده و از ایده‌آل سرعت به شدت بکاهد، تا حدی که ارتباط TCP به کل مختل میشود . از سمت دیگر به واسطه ترافیک کمی که این حمله تولید می‌کند تشخیص رخداد آن بسیار مشکل میشود .