

عنوان مقاله:

روش های شناسایی و مقابله با حملات DDoS در لایه های مختلف OSI

محل انتشار:

کنفرانس ملی فناوری های نوین در مهندسی برق و کامپیوتر (سال: 1396)

تعداد صفحات اصل مقاله: 20

نویسندگان:

فرهنگ پدیداران مقدم - استادیار گروه کامپیوتر، موسسه آموزش عالی اشراق بجنورد

حمید مقصودی - دانشجوی کارشناسی ارشد، موسسه ی آموزش عالی اشراق بجنورد

خلاصه مقاله:

هدف از ارایه این مقاله پژوهشی، تشریح حملات انکار سرویس DoS و حملات انکار سرویس توزیع شده DDoS و نحوه شناسایی و مقابله با آنها است. این پژوهش در قالب شناسایی حملات در لایه های 3 و 7 و 4 مدل مرجع OSI تمرکز دارد. در ابتدا حملات DDoS و DoS را به طور خلاصه معرفی میکنیم. در قسمت بعدی، روش های کشف و مقابله با حملات DDoS در لایه شبکه و کاربرد را بررسی میکنیم. سپس یک چهارچوب مبتنی بر PCA برای شناسایی حملات DDoS لایه ی کاربرد را معرفی خواهیم کرد. در قسمت سوم، کشف حملات DDOS با استفاده از تخمینگر های فازی بلادرنگ در لایه شبکه را تشریح میکنیم. در قسمت نهایی نیز شناسایی حملات DDoS در ابعاد گسترده اینترنتی که در آن کاربران قربانی نقش ایفا میکنند را مورد بررسی قرار می دهیم.

کلمات کلیدی:

حملات DDoS لایه کاربرد سیل، HTTP امتیاز اتصال ConnectionScore App-DDoS شناسایی نابهنجاری، رفتار بروزینگ کاربر، ترافیک شبکه، چهارچوب تحلیل اولیه PCA ترتیب متوالی مستقل، خوشه بندی

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/758760>

