

عنوان مقاله:

Analysis and Detecting TCP SYN flood attacks based on kernel-events in Cloud Computing

محل انتشار:

کنفرانس بین المللی مهندسی کامپیوتر و فناوری اطلاعات (سال: 1395)

تعداد صفحات اصل مقاله: 8

نویسندگان:

Hossein Abbasi - *Computer Engineering Department, École Polytechnique de Montréal. Montreal, Canada*

Chamseddine Talhi - *Department of Software Engineering and Information Technologies École de technologie supérieure , ETS, Montreal, Canada*

خلاصه مقاله:

Security is one of the most important challenges in cloud computing as there are a lot of threats and attacks which put the security of a cloud in risk. One of the most common attacks to cloud computing is DDoS (Distributed Denial of service) attack. The absolute prevention of the occurrence of DDoS attacks is not possible; therefore, detecting these attacks is an important step in securing a cloud against this kind of very common security threat. The attacker in DDoS attack tries to flood a target machine with sending packets similar to normal and factual traffic sent by another virtual machine. Therefore the detection systems cannot successfully detect DDoS attacks. On the other hand, distributed nature of these attacks makes them more difficult to be detected. In this paper we propose a model to detect Transmission Control Protocol Synchronize (TCP SYN) flood attack as a very popular type of DDoS attacks.

کلمات کلیدی:

Cloud Computing; Security; DDoS; TCP SYN flood

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/493980>

