عنوان مقاله:
مطالعه و ارزیابی روش های سیستم تشخیص نفوذ

محل انتشار:
همایش دستاوردهای نوین در هوافضا و صنعت هواپیمایی ایران (سال: ۱۳۹۶)

تعداد صفحات اصل مقاله: ۱۶

نویسنده:
سید محسن هاشمی - دانشگاه آزاد اسلامی واحد بروجرد

خلاصه مقاله:
رشد روز افزون استفاده از خدمات شبکه های کامپیوتری از یک سو و حمله به شبکه کامپیوتری از سوی دیگر باعث شده است که سیستم های تشخیصنفوذ به یک زمینه تحقیقاتی مهم در مسیله امنیت سیستم های کامپیوتری تبدیل شود. سیستم های تشخیص نفوذ برای کمک به مدیران امنیتی سیستمدر جهت کشف و حمله به کار گرفته شده اند. برای ایجاد امنیت در سیستم های کامپیوتری، علاوه بر دیواره های آتش و دیگر تجهیزات جلوگیری از نفوذ، سیستم های دیگری به نام سیستم های تشیی نفوذ (IDS) مورد نیاز می باشند تا بتوانند در صورتی که نفوذگر از دیواره ی آتش، آنتی ویروس و دیگر تجهیزات امنیتی نفوذ کرده و وارد سیستم شد، آن را تشخیص داده و چاره ای برای آن بیاندیشد. بنابراین، هدف یک سیستم تشخیص نفوذ، جلوگیری از حمله نیست و تنها کشف و احتمالا شناسایی حملات و تشخیص اشکالات امنیتی در سیستم یا شبکه کامپیوتری و اعلان آن به مدیر سیستم است. سیستم های تشخیص نفوذ را می توان از سه جنبه روش تشخیص ، معماری و نحوه پاسخ به نفوذ طبقه بندی کرد. انواع روش های تشخیص نفوذ عبارت اند از تشخیص رفتار غیرعادی و تشخیص سوء استفاده (تشخیص مبتنی بر امضاء). الگوریتم های مختلفی برای مشخص نمودن جریان نرمال از جریان غیر نرمال است. با در نظر گرفتن موارد گفته شده، در این سمینار، به مطالعه و ارزیابی روش های ارایه شده برای تشخیص نفوذ پرداخته و بصورت جامع بحث تشخیص نفوذ را مورد بررسی قرار داده ایم.

کلمات کلیدی:
(DIDS)) Distributed Intrusion Detection System ، (NIDS) Network-based Intrusion Detection System ، HIDS) Host-based Intrusion Detection System