مجله رویکردهای نوین در تحقیقات علوم پایه، فنی و مهندسی
سال اول، شماره ۲، بهمن ۱۳۹۷
ISSN: ۲٦٤٥-٥٤٣٩
www.jonarbset.ir

Honeypot در امنیت شبکه

پریسا آزاده ، مهشید قاهری تبریزی ، فرشید صهبا

چکیده

شبکه رایانه‌ای و اینترنت هر روز در حال گسترش هستند. شبکه‌های کامپیوتری به کاربر اجازه دسترسی به پایگاه داده‌های محلی و دوردست را می‌دهند. شبکه و امنیت در صنایع موضوعات مهمی هستند؛ چون نقص در سیستم می‌تواند موجب مشکلات عمده‌ای شود. سیستم تشخیص نفوذ (IDS) برای نظارت بر فرآیندهای یک سیستم یا یک شبکه جهت بررسی تهدیدات استفاده می‌شود و به مدیر شبکه حمله را هشدار می‌دهد. IDS تنها برای صنایع با مقیاس بزرگ راه‌حل ارائه می‌کند، اما هیچ راه‌حلی برای صنایع با مقیاس کوچک وجود ندارد؛ بنابراین مدل Honeypot برای حل مشکل صنایع با مقیاس کوچک پیشنهاد شده است. تعریف Honeypot کار سختی است، چراکه آن‌ها در پیشگیری، تشخیص، جمع‌آوری اطلاعات و کارهای دیگری مورد استفاده قرار می‌گیرند، اما حالت دفاعی ندارند و به عبارتی کار امنیتی نمی‌کنند اما بر امنیت شبکه به شدت تأثیر می‌گذارند. این مدل، فعالیت‌های مهاجمان را ثبت می‌کند و برای تمام این فعالیت‌ها یک log نگه می‌دارد. تمرکز این مقاله جلوگیری از حملات مهاجمان خارجی و داخلی و حفظ فایل لاگ با استفاده از honeypot به‌وسیله ماشین مجازی است.

واژه‌های کلیدی: Honeypot، log، IDS