УДК 621.391

СИСТЕМА ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ IPS/IDS

Каплич А.А., магистрант гр. 967001

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шевчук О.Г.. – канд. тех. наук, доцент

Аннотация. *Описаны системы обнаружения и предотвращения вторжений в сетевую инфраструктуру.*

Ключевые слова. Система обнаружения вторжений, система предотвращения вторжений, IPS, IDS.

Рассмотрим такой класс решений, как системы обнаружения вторжений и системы предотвращения вторжений. Данный класс средств защиты нацелен на выявление и регистрацию недостатков в безопасности внутренней инфраструктуры – сетевые атаки, попытки несанкционированного доступа, повышения привилегий, работа вредоносного ПО и т.д.

IDS состоит из сенсоров, которые просматривают сетевой трафик или журналы и передают анализаторам, анализаторы ищут в полученных данных вредоносный характер и в случае успешного обнаружения – отправляет результаты в административный интерфейс [1]. В зависимости от места расположения IDS делятся на сетевые (network-based IDS, NIDS) и хостовые (host-based, HIDS). В свою очередь IPS это программная или аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них. Методы ее работы относятся к своевременным (превентивным) и проактивным, в отличие от IDS, выполняющей детективные функции. Возможность предотвращения атак реализована за счет того, что сетевая IPS, как правило, встраивается «в разрыв» сети и пропускает через себя весь трафик, а также имеет внешний интерфейс, на который приходит трафик и внутренний интерфейс, который пропускает трафик далее, если он признается безопасным [2]. Структурна схема IPS/IDS представлена на рисунке 1.

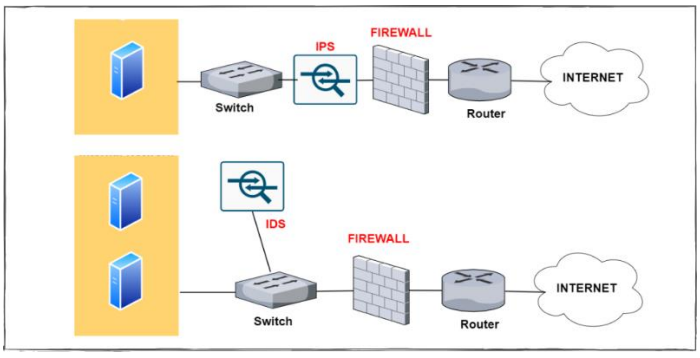

Рисунок 1 - Структурна схема IPS/IDS

Наиболее эффективной защиты инфраструктуры является совместное использование средств IDS и IPS в одном продукте – межсетевом экране, который с помощью глубокого анализа сетевых пакетов, обнаруживает атаки и блокирует их. Стоит отметить, что речь идет только об одном рубеже защиты, который, как правило, расположен за межсетевым экраном. И чтобы добиться комплексной защиты сети, необходимо использовать весь арсенал средств защиты, например,

UTM (Unified Threat Management) – совместно работающие межсетевой экран, VPN, IPS, антивирус, средства фильтрации и средства антиспама [3].

Список использованных источников:

1. Kruegel Christopher, Valeur Fredrik, Vigna Giovanni // Intrusion Detection and Correlation: Challenges and Solutions. 2005. P. 43–55.

2. Лукацкий А.В. // Обнаружение атак. 2001. P. 247–286.

3. Норткат С., Новак Д. // Обнаружение нарушений безопасности в сетях. 2003. P. 161–185.

INTRUSION DETECTION, PREVENTION SYSTEM

Kaplich A.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Shevchuk O. G. – PhD in Technical, docent

Annotation. The systems for detecting and preventing intrusions into the network infrastructure are described.

Keywords. Intrusion detection system, intrusion prevention system, IPS, IDS.