Investigation of the Intrusion Detection System “Snort” Performance

N. Paulauskas, J. Skudutis
Department of Computer Engineering, Vilnius Gediminas Technical University,
Naugarduko str. 41, LT-03227, phone +370 5 2744767; e-mail: nerijus.paulauskas@el.vgtu.lt; julius.skudutis@el.vgtu.lt

Introduction

With the increasing dependence of the world economy, state structures, communications, industry and business on information technologies, the risk related to the ever pervasive intrusions in the electronic space also increases. Malicious intruders overcome protection systems, designed to limit access to the institution computer network resources installed in banks or companies. In order to reduce the risk and possible consequences, it is very important to identify intrusions at the initial stage of their realization and to respond to them appropriately [1, 2]. For this purpose the intrusion detection systems can be applied. The intrusion detection system (IDS) is a protection system intended to identify and to respond to the malicious activities directed against the computer and computer network resources.

The intrusion detection systems are most often classified according to the two features: according to technologies used for the intrusion detection and according to the practical implementation of IDS systems, i.e. according to the monitored object [3, 4]. According to the technologies used to detect incidents the intrusion detection systems are divided into systems in which signature- or anomaly-based methods are applied [5, 6].

According to the monitored object two types of intrusion detection systems are distinguished: Host IDS and Network IDS. Host IDS – (HIDS) is the system detecting intrusions directed against a concrete network host. Network IDS – (NIDS) is the system detecting intrusions directed against the whole network or the network segment.

It is important that the intrusion detection system should process all packets transmitted over the network irrespective of the network usage, i.e. it is necessary to reduce the number of dropped packets to the minimum.

The aim of this work is to investigate the performance of the recent most popular open source network intrusion detection system Snort 2.8.0 (which became the intrusion detection standard de facto), its dependence on the hardware and the chosen logging way of alerts about intrusions as well as to provide recommendations to the system user how to improve the system performance and make the best possibilities.

Intrusion detection system Snort

Snort appeared as a simple packet sniffer program, which was later developed into the intrusion detection system. Snort’s architecture consists of four basic components: the packet decoder, the preprocessor, the detection engine and the alerts/logging module. The data packet enters the system through the network interface card and the packet capture module. In the packet decoder, the packet protocol is determined and it is checked if the packet data match the protocol. The packet decoder can generate the message itself in case the packet header is malformed, the packet is too large, unusual or improperly indicated protocol parameters in the packet header, etc.

Then the packet is transmitted to preprocessors. Preprocessors are additional Snort modules allowing checking of the data in different ways. Each of Snort preprocessors performs a particular task, e.g.: tracks the flow (flow), reassembles the stream (stream5, frag3), detects the port scan (sfsPortscan), checks the application level protocols such as FTP, Telnet, SMTP. As soon as preprocessors finish their operation, the packet is transmitted to the detection engine, which compares the packet flags with those described in the rules. Lastly, the packet is transmitted to the output registration and information modules which generate the alert about the intrusion.

The Snort speed at which the network packets are sniffed and processed depends on the number of used preprocessors and rules according to which the packets are checked and processed. In order to avoid the dropping of packets, it is necessary that the intrusion detection system should be able to process all packets transmitted over the network.

The main hardware components having influence on the intrusion detection system performance are the CPU, memory, the system bus, the network interface card (NIC) and a hard disc [7].

In the IDS sensor the highest-speed financially feasible processor should be implemented. It should be
known that a processor is a critical component but it is
good as the weakest out of 5 mentioned system components is good.

Investigation methods

During the investigation two computers interconnected by the twisted pair cable were used. One of
the computers was intended to send the network traffic, while in the other computer the intrusion detection system
Snort 2.8.0 was implemented (Fig. 1). The dependence of

the intrusion detection system Snort 2.8.0 performance on the hardware and the chosen technique of logging alerts
about intrusions was investigated.

Snort 2.8.0 was implemented in computers of different performance (Table 1). Investigations were
carried out with default settings of the Snort 2.8.0 program preprocessors and rules. The perfmonitor preprocessor

\[\text{CPU: } \text{PentiumIV, 3200 MHz} \quad \text{PentiumIII}, 1800 \text{ MHz} \quad \text{PentiumIII, 450 MHz} \]
\[\text{RAM: } 2 \text{ GB} \quad 256 \text{ MB} \quad 128 \text{ MB} \]
\[\text{HDD: } 16 \text{ GB, 7200 RPM, SATA-II} \quad 40 \text{ GB, 7200 RPM, Ultra-ATA/133} \quad 10 \text{ GB, 5400 RPM, Ultra-ATA/66} \]
\[\text{Integrated NIC: } \text{Marvell, Yukon 88E8001/8003/8010 PCI Gigabit Ethernet Controller} \quad \text{Intel(R) PRO/100 VE Network Connection} \]
\[\text{NIC: } \text{a. Intel PRO/1080 GT PWL8391GT (1, 2, 3 computers)} \quad \text{b. Intel PRO/1000 PT EXP93000P/TBLK (1 computer)} \quad \text{c. Realtek RTL8139 Family PCI Fast Ethernet NIC (1, 2, 3 computers)} \]

intended for collection and registration of statistics about
the program operation was additionally enabled. This
preprocessor presents data about the system load, received and
dropped packets, the network usage, etc. During the investigation the Snort 2.8.0 rulesets of 9 October, 2007
was used. According to the default program settings, packets transmitted over the network were checked
according to 6715 rules. Data about intrusions were logged in 2 ways: a) saved by the Snort program in the MySQL
5.0.45 data base; b) saved in the file in a unified binary format and then using Barnyard 0.2.0 tool sent to the
database (Fig. 1). Using the second way, the Snort 2.8.0

system does not have to waste time for SQL query formation, data sending to the database and receiving
answers about the query execution. For the packet capture, the Libpcap 0.9.8 packet capture library was used.

The intrusion detection system Snort 2.8.0 was implemented in the Linux type operating system. There
were some reasons for the system selection: Linux type OS is the most widely used system in implementing
Snort, besides the Snort creators themselves recommend using Linux or BSD type OS in IDS sensors
[7]. Slackware 12.0 distribution operating on the 2.6.21.5
version core basis was chosen.

For investigations the network traffic of the VGTU
Computer engineering department was applied. This traffic
was captured in the daytime when the network usage is the
largest. During the traffic capturing, for generation of the
additional malicious network packets, the recent best
estimated vulnerability scan tool Nessus was used. The
network traffic was captured using the packet sniffing and
logging tool Tcpdump.

The main parameters of the network traffic used in
testing were:

- The number of packets: 1000000, out of which
  99.36% tcp, 0.37% udp, 0.07% icmp;
- average data transmission rate: 6.707 MBit/sec;
- average packet size: 724 bytes;
- average number of packets per second: 1157.371;
- duration: 864.027 seconds.

For the traffic replay back to the network the

Tcpreplay program was used. This program allows
choosing the traffic replay rate. In this way it can be
investigated how the intrusion detection system Snort 2.8.0
processes the same network packets sent at a different rate,
how the intrusion detection results change by varying the
IDS system configuration parameters, etc.

Investigation results

The investigation results of Snort 2.8.0 implemented in
the system with the PentiumD processor are presented in
Fig. 2. The dependence of the number of dropped network
packets by the system on the packet sending rate is shown
in this figure. Curves 1, 2, 3 and 4 show the results
obtained using different network interface cards.

The figure also shows that by sending network
packets at a rate not higher than 50 Mbps, the system
manages to process all packets transmitted over the
network irrespective of the used network interface card.

![Fig. 2. Investigation results of Snort 2.8.0 with PentiumD processor and different network interface cards: 1 – c (see Table 1); 2 – a; 3 – b; 4 – integrated; 5 – a, when Barnyard 0.2.0 was used for data logging](image-url)
Differences appear when packets are transmitted at the rate higher than 50 Mbps. The largest number of packets is dropped with the network interface card having a Realtek RTL8139 controller, the least – with the Intel PWL8391GT network interface card.

Curves 1, 2, 3 and 4 were obtained when the Snort 2.8.0 system itself import data about intrusions in the MySQL database. Better results are obtained by logging data in a second way (using Barnyard 0.2.0 tool). In this case, the number of dropped packets does not exceed 0.08% (Fig. 2, curve 5).

The investigation results of Snort 2.8.0, the system with the Pentium IV processor, are presented in Fig. 3. The comparison of these results with those presented in Fig. 2 shows that packets are dropped much earlier, i.e. reaching the traffic transmission rate of 30 Mbps (1, 2, 3 and 4 curves). The difference between the number of dropped packets using different network interface cards appears when the traffic is transmitted at the rate higher than 70 Mbps.

Already in the Snort 2.6 version, for the packet checking according to rules a new aho-corasick pattern-matching algorithm is applied, which changed the earlier used wa-manner algorithm. The Aho-Corasick algorithm is faster but it uses more RAM of the system. According to default settings, Snort 2.8.0 uses the aho-corasick algorithm.

The investigation results of the intrusion detection system Snort 2.8.0 with the Pentium III processor are presented in Fig. 4. It can be seen from this figure that when the traffic sending rate reaches 45 Mbps, the system drops more than 50% of all packets transmitted over the network. Even after changing the network interface cards and the pattern-matching algorithm, the results did not improve. Curves 4 and 5 show the results obtained by logging alerts in a file in a unified binary format.

![Fig. 3. Investigation results of Snort 2.8.0 with Pentium IV processor and different network interface cards: 1 – c; 2 – c and lowmem pattern-matching algorithm; 3 – integrated; 4 – a; 5 – a, Barnyard 0.2.0 was used for data logging.](image)

In systems with a little amount of random access memory instead of this algorithm a lowmem algorithm using less random access memory can be chosen. The investigation results of the intrusion detection system with the Pentium IV processor and random access memory of 256 MB are shown in Fig. 3, curves 1 and 2. These results were obtained by using different pattern-matching algorithms. Curve 1 was obtained by applying the aho-corasick algorithm, and curve 2 – the lowmem algorithm. As can be seen in Fig. 3, when applying the lowmem algorithm, better results are obtained only when the traffic sending rate is higher than 70 Mbps. When the network packet sending rate is lower, irrespective of the chosen pattern-matching algorithm, the number of dropped packets does not change. Curve 5 confirms the above mentioned conclusions that when the system load is lower its performance is better.

![Fig. 4. Investigation results of Snort 2.8.0 with Pentium III processor obtained with the c type network interface card using different pattern-matching algorithms: 1 – lowmem; 3 – aho-corasick; and with the a type network interface card using different data logging ways: 2 – Snort to MySQL; 4 – Snort and Barnyard 0.2.0; 5 – Barnyard 0.2.0.](image)

The difference is that in the first case Snort 2.8.0 and Barnyard 0.2.0 programs were operating at the same time, while in the second case (curve 5) only Snort 2.8.0 was operating and alerts were logged only in a file. Data were sent to the database after finishing the analysis of the sent traffic. As can be seen in Fig. 4, in this case the results improve slightly.

Diagrams of the intrusion detection CPU usage are presented in Fig. 5. Results were obtained using the Intel PRO/1000 GT PWL8391GT network interface card and Barnyard 0.2.0 program. The test of the CPU usage allows checking if the processor speed is sufficient to process the traffic. As indicated in [7], when the system is idling and no packets are being accepted or analyzed, the processor usage should not exceed 2-3%. By analyzing the traffic, the sending rate of which is equal to 25% of the network bandwidth, the processor load should not exceed 15%. When the traffic reaches 50% of the network bandwidth, it is important that the processor usage should be lower or equal to 45%.

![Fig. 5. Diagrams of intrusion detection system CPU usage: 1 – Pentium III; 2 – Pentium IV; 3 – Pentium D.](image)
As can be seen in Fig. 5, in the systems with PentiumIV and PentiumD processors (curves 2 and 3), the processor performance satisfies the above mentioned conditions, and the processor of the system with the PentiumIII processor (curve 1) is maximally loaded when the rate of the traffic exceeds 30 Mbps, therefore the number of dropped packets considerably increases by further increasing the packet sending rate (Fig. 4).

Conclusions

The investigation results have shown that hardware and alerts logging technique are the main factors having impact on the intrusion detection system Snort 2.8.0 performance.

The system operates best with the PentiumD processor. When the network traffic rate does not exceed 50 Mbps, the performance of the system is good and it manages to process practically all packets transmitted over the network irrespective of the chosen network interface card or logging alerts technique. The number of dropped packets in the whole investigated rate range (up to 100 Mbps) was ≤ 0.7%, and when alerts were logged in a database using Barnyard 0.2.0 it was ≤ 0.1%.

The intrusion detection system Snort 2.8.0 with the PentiumIV processor begins to drop packets already at the transmission rate of 30 Mbps. The network interface card and the pattern-matching algorithm have influence on the number of dropped packets in this system only when the traffic rate exceeds 70 Mbps. When Barnyard 0.2.0 is used to log alerts in the database, the number of dropped packets is ≤ 0.7%.

The system with the PentiumIII processor in 100 Mbps network is not suitable for the intrusion detection because when the traffic sending rate reaches 45 Mbps, the system drops more than 50% of all packets transmitted over the network.

References


Received 2008 03 05


Possibilities of the intrusion detection system Snort and factors influencing its performance are considered in the work. For this purpose the dependence of the system Snort 2.8.0 performance on the chosen hardware and the technique of logging data about intrusions has been investigated. It is shown that the number of dropped packets is a very important factor having impact on the system performance. The main factors having influence on the system performance are determined and recommendations allowing improvement of intrusion detection are presented III. 5, bibl. 7 (in English, summaries in English, Russian and Lithuanian).


Исследуются возможности системы обнаружения вторжений „Snort“ и факторы, влияющие на ее эффективную работу. С этой целью исследована зависимость производительности системы „Snort“ от выбранной аппаратуры и метода регистрации данных об атаках. Показано, что очень важным фактором, влияющим на эффективность работы системы, является количество потерянных пакетов. Определены основные факторы, влияющие на количество потерянных пакетов и даны рекомендации, позволяющие повысить эффективность работы, системы обнаружения вторжений „Snort“. Ил. 5, bibl. 7 (на английском языке, рефераты на английском, русском и литовском яз.).


Nagrainejame atakų atpažinimo sistemas Snort galimybės ir jos efektyvų darbą sąlygojantys veiksniai. Tam tikslui išsirita sistemos Snort 2.8.0 našumo priklausomybė nuo pasirinktos aparatūros įrangos ir duomenų apie atakas registravimo būdo. Parodyta, kad iš tikrų svarbus veiksmai, turintys įtakos sistemos darbo efektyvumui, yra pamestų paketu įskaičius. Atskleisti pagrindiniai sistemos efektyvumui įtakos turintys veiksmai ir pateikti rekomendacijos, kaip pagerinti atakų atpažinimo sistemos darbo efektyvumą. Išl. 5, bibl. 7 (anglų kalba, santraukos anglų, rusų ir lietuvių k.).