Framework for Choosing Best Intrusion Detection System

Bilal Maqbool Beigh

Submitted in February, 2014; Accepted in November, 2014

Abstract - As there are many intrusion detection systems available in the market and yet there is not a single guideline framed by any researcher or any organization so that a company or an organization will decide which intrusion detection system is best suited to their company for the purpose of security. Here in this paper, we have proposed a novel guideline in terms of framework for choosing right most intrusion detection system for an organization. The framework needs some security expert so that they can check the equation to be satisfied.

Index Terms – Framework, Guideline, model, IDS, Intrusion.

1.0 INTRODUCTION

The story of the human life started with Stone Age, then agriculture age and now we are in the information technology age, where everything depends upon information and information processing systems. Information ranging from personnel to commercial have been processed and exchanged by these information systems. With the advent of Internet, the convergence of information & communication technologies and today's very complex nature of business environment resulted in myriad trust and information security concerns. The secure functioning of these information systems is the utmost important and foremost concern. Information security is a field of security which ensures the confidentiality, integrity and availability of information and information processing resources. Many security professionals think that developing a completely secure system is almost an impossible task. According to [1] the completely secure system is one that is disconnected from a network, encased in concrete, and lying at the bottom of the ocean. In this networked environment where there are potential number of hackers and adversaries present, security enforcing mechanisms needs to be incorporated in the information systems to with stand with the both deliberate and accidental malicious intents. Hence this tremendous growth in communication technology brings number of good things to human society, but it also makes us re-lay on information systems [2].As the information is increasing in digital format day by day, the vulnerabilities are also increasing in the form of cyber threats, attacks and mis-identification of trusted users. There are lots of intrusion attacks in today's digital world, according to recent survey by CERT/CC [3], the rate of intrusion attacks almost doubles every year.

P. G. Department of Computer Sciences, University of Kashmir, Jammu and Kashmir, INDIA
E-mail: bilal.beigh@gmail.com

The Computer Emergency Response Team (CERT) reported 3734 incidents in 1998, 9859 in 1999 and 8836 in the first 6 months of 2000. In a recent audit of U.S. federal agencies by the GAO [4] investigators were able to pierce security at nearly every system they tested. The cause of these attacks are either complexity of the system itself or increasing number of hackers day by day or market competitors or software development companies itself etc. Therefore along with these tremendous opportunities for sharing important information and resource especially used for some critical operation like military , space, nuclear etc. It has become very much important to protect these special and important resources and information against such attacks [5]. For protecting the same, we have the concept called "Information security" thus we can say that information security is such area which protects our information / resources from theft or misuse. But still this field of research is in its infancy days. This research started in early 90's and so far little has been done in this field. This research field comprises of many subfield such as system side security, network side security etc. One subset of information security that has been the area of much more attention in recent years is intrusion detection system [5]. Therefore intrusion detection system can be defined as the process of monitoring events occurring in a system and signaling responsible parties when interesting (suspicious) activity (compromises the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network) occurs [7]. At this instant of time, there are many intrusions detection systems available in market with different features and uses, but it is very difficult for a user or organization to choose best Intrusion detection system for him or for his organization [8][14]. As there is no such guideline provided by any agency/ organization to choose the security policy therefore there is a need of guidelines for the purpose. Here In this research work, we will provide a framework in terms of mathematical equations and steps for choosing best possible intrusion detection system for you and your organization. This part will ensure that the system for intrusion detection should be made in accordance to the model prepared in terms of equations and physical model to be described in the next sections of this paper.

2.0 NEED FOR FRAMEWORK FOR CHOOSING IDS

The intrusion detection system allows us to make the system safe from the most attackers. Thus as described in previous and this chapter, intrusion can be defined as a process of accessing someone's personal property or data or information without proper access or proper authentication cardinalities. As all of us know that today's almost 90 percent of information is available online through websites or computer programs. Although this make very ease and very fast access to the people overall the

globe, but it also increases the risk to the maximum. According to Symantec report, around 1, 00,000 websites are available online and some of them share the critical information and valuable data. In order to steal the critical data or important and relevant information without having legitimate access to the resources, the person on longer need not to be a hacking gem, just download and run the hacking program, make some settings and you are done [9][16]. In order to secure the companies or individual's data/ information, firewalls are being installed, but they alone do not serve the purpose of defending the data from attacks or intruders. The main aim of the firewall is to filter the traffic but they cannot block all the traffic. Also once the traffic passed through the firewall there is no such mechanism available that traffic will be monitored inside the network for rest processing. Also firewall only detects external traffic coming to it, but doesn't detect the internal attacks. By using intrusion detection system, we can monitor or do the following things:

- Monitors network traffic.
- Continuously monitors servers/ network for misuse actions or abuse policy.
- Attack / breach alerting, response and reporting.
- Countermeasures.

Thus it became very much important for an organization to install both firewall and intrusion detection system to secure their assets / information for hackers / attackers. Also for securing this particular data and information from the attackers, there are lots of intrusion detection mechanisms currently available in the market. Every intrusion detection manufacturing organization highlights his qualities of making secure the information, but none of the organization or research community describes the guidelines for picking the most appropriate and good suitable intrusion detection system for any company or individual. Thus it became very much important to provide some guidelines either through some model or through some mathematical formula to suggest the company which intrusion detection system is most suited for them and under which norms. We have taken a step towards the development of guidelines for choosing the right intrusion detection in accordance to their requirements and importance's. In this chapter we have presented guidelines for choosing right most intrusion detection system for company or individual under required condition. The guidelines will be discussed in next section of this chapter.

3.0 FRAME WORK FOR CHOOSING INTRUSION DETECTION SYSTEM

Choosing an intrusion detection system is a delicate task, as the whole company security responsibility lies on the shoulders of the intrusion detection system i.e.to detect the attack made on the organization system, to mitigate them if possible or to alert the administrator about the attack happened [4]. Currently there are many intrusion detection systems available within the market but it is difficult to choose the best intrusion detection system for an organization[17]. In order to choose the same, we have devised a framework that will help an organization to choose the best intrusion detection. The framework consists of logical steps and which when followed revealed the desires intrusion detection system. The steps which are involved in choosing best intrusion detection are as:

- Risk Analysis.
- Detection Rate
- False Alarm Rate
- Cost Benefit analysis
- Updates or patches ratio.

When the above mentioned steps are followed in a manner shown in figure below (cc), yield the results based on the mathematical formulas. The accepted criteria must be decided by the security professionals to choose best intrusion detection system.

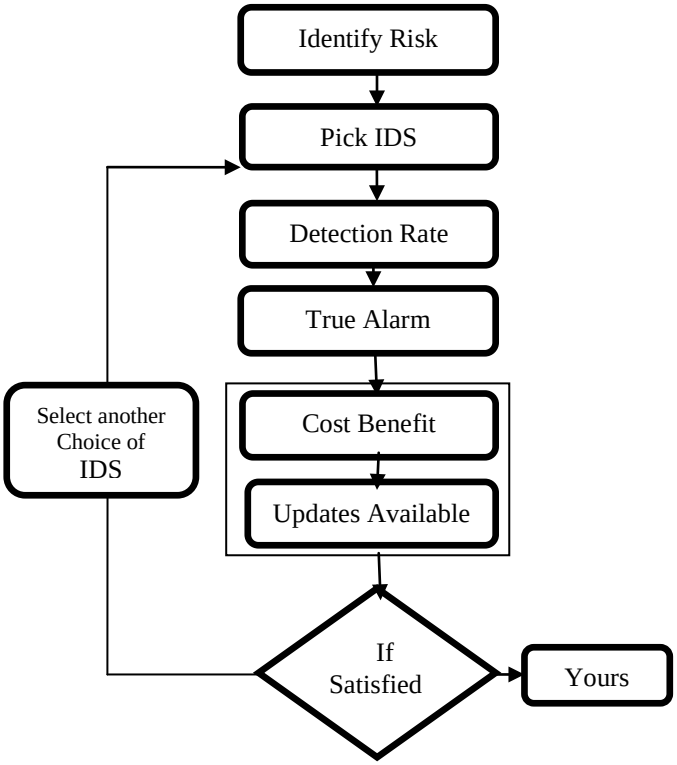

Figure 1: Frame Work for choosing right intrusion detection system

3.1 Risk Analysis

The Risk analysis step is the first step towards the choosing of intrusion detection and prevention system for an individual or an organization. This step is most important and critical towards the picking of right most intrusion detection system. The risk calculation is very big thing to do because it deals with the overall security of the organization. The risk analysis can be considered as a tool for risk management, which is helpful for identifying security issues i.e. vulnerabilities, threats and unauthorized access. Also as per the general definition of risk on different blogs and websites, the risk can be calculated as:

"Risk = Threats x Vulnerabilities x Impact"

But we have devised the risk in accordance to our own formulas. The formula will depend upon the following factors.

i. Summation of threats.
ii. Value / impact of threats
iii. Total Impact of assets under risk
iv. Total assets of the organization.

Before enforcing the formula, The RAG (Risk Analysis Group) will find two important aspects used in making the formula which are [10] [11] [12] [13]:

- Identifying important information and their Values
- Identifying threats and Vulnerabilities for the assets

Identifying important information and their Values – Identifying the values of the organization's important information is the very first step for risk analysis. In this step the risk assessment group will point out / identify the most important assets of organization and will estimate the cost associated and damage resulted if some intrusion/ attack happed on an organization or we can say the group will analyze the loss made by losing the information to some other company. While identifying the assets following things must be kept in consideration.

- Cost of assets/ information that may be lost if intrusion happen.
- Role and usage of assets / information.

Identifying threats and Vulnerabilities –After pointing out the important information/assets, the responsibility of the group is to identify the vulnerabilities and threats for assets/ important information as identified in the prior step. Also they have to keep an order of threats i.e. which threat may damage/ theft more information according to the percentage of damage done by these threats and vulnerabilities. Thus in general, the RAG will gather the information about the loss of assets / information in total at the initial stage, if not prevented and total threats and vulnerabilities that can cause these losses. After acquiring the above two steps, we have derived a formula which we are going to use to calculate the risk is as under:

$$\text{Estimated Risk} = \sum_{i=1}^{n} \text{P(Assetsaffectedbythreats} * \text{valueoftheassets)}$$

$$\text{wherepisprobablityof}$$

By calculating the estimated risk, we can have idea about how much it will affect our assets. Therefore the overall percentage of the risk can be calculated with the help of the following formula.

$$\text{Risk} = \frac{\text{Total Assets of the organization} * \text{vlaue of assets}}{\text{Estimated Risk}} * 100$$

After getting the results of assets under risk in percentage, we will move towards the next step of the frame work.

3.2 Picking of IDS

Every organization wants to secure their confidential resources, for that they have to make some selection in terms of firewalls, IDs etc. Before going for any products, the company should consider all the available resources for basic system operation and maintenance. Thus should be able to pick the appropriate IDS which will meet the needs within the constraints laid down by company. This task is very difficult, As there is no industry standard against which we will compare IDS. Hence there is a need of providing a standard benchmark for IDS. The new product cycle for commercial IDSs is rapid, and information and systems quickly become obsolete. Steven Northcutt recommends the use of product guides that are updated at least monthly. Relatively little objective third party evaluation of IDSs is available, while trade press reports are generally spotty and superficial. Setting up a facility to objectively compare IDSs will be prohibitively expensive for all but the largest potential users, and some third-party or industry sponsored effort is needed. Marketing literature rarely describes how well a given IDS finds intruders and how much work is required to use and maintain that system in a fully functioning network with significant daily traffic. IDS vendors usually specify which prototypical attacks their systems can find, but without access to deployment environments, they cannot describe how well their systems detect real attacks while avoiding false alarms. Edward Amoroso and Richard Kwapniewski recently provided guidance in selecting IDS [14] by making some questionnaires, upon the receiving the answers from the users, they will choose the intrusion detection system. These guidelines have impact of bias towards a particular intrusion detection system. This step is very important, as it is concern with the security of overall system. The step choice based and will not be entertained in the conditions which are going to decide that is the picked intrusion detection system the right most intrusion detection for their organization. The decision of this step lies on the shoulders of the Risk analysis group. They are the security professionals which will decide the most suited as per the threats and vulnerability of the organizations.

3.3 Detection Rate

The step is very much important as the decision is concerned. The detection rate for a particular intrusion detection system will be available in the literature and papers available in different research journals. Let us make an example, in one of our experiment, the snort has detection rate of 99.4 % which means that 99.4% of attacks are being detected by the snort coming towards the system. Similarly all intrusion detection has the documentation, which shows the rate of detection for that intrusion detection system. Rate of detection can be calculated as:

$$\text{DR} = \frac{\text{Detectedattackscommingtowardsthesystem}}{\text{Totalno. ofattackscommingtowardsthesystem}} * 100$$

Or we can say that the rate of detection can be calculated as:

$$\text{DR} = \frac{\text{TP}}{(\text{TP} + \text{TN})} * 100$$

TP = amount of attack when it actually attack
TN = amount of normal detect when it actually normal
Also rate of detection can be calculated using the above formula. The detection rate is very much important as per selection is concerned. It shows the overall rate. If the detection rate is greater than 90 %, the system is partially accepted. Which means the system will be evaluated for the next section. i.e. True alarm Rate .

3.4 True Alarm Rate

The step is much important as per the decision is concerned. As we are calculating the rate of false positive alarm rate which can be calculated as the ratio of in-correct classified intrusions to the total number of normal records. Therefore false positive rate (FPR) can be calculated as:

$$\mathrm{FPR} = \frac{\sum \mathrm{FalseAlarm\ Detected}}{\sum \mathrm{Totalnumberofrecords}} * 100$$

But we have to calculate the True Positive alarm rate which can be derived as from the above formula, which can be derived as below:
True Positive Rate = 100- false Positive Rate
Let us assume we got the false positive rate as 3.06% , then we can easily get the true positive rate as 96.77% which means that the system is accurately identifying 96.77 % of the intrusions that of total available in the dataset. Upon partial accepted from previous sections. If the true alarm rate is less than 95 %, it is partially accepted.

3.5 Cost Benefit Analysis.

There is a variety of approaches to cost analysis, the suitability of any of which depends upon the purpose of an assessment and the availability of data and other resources. It is rarely possible or necessary to identify and quantify all costs and all benefits (or outcomes), and the units used to quantify these may differ.
Main types of cost analysis include the following.

- Cost-of-illness analysis: a determination of the economic impact of an illness or condition (typically on a given population, region, or country) e.g., of smoking, arthritis or bedsores, including associated treatment costs
- Cost-minimization analysis: a determination of the least costly among alternative interventions that are assumed to produce equivalent outcomes.
- Cost-effectiveness analysis (CEA): a comparison of costs in monetary units with outcomes in quantitative non-monetary units, e.g., reduced mortality or morbidity.
- Cost-utility analysis (CUA): a form of cost-effectiveness analysis that compares costs in monetary units with outcomes in terms of their utility, usually to the patient, measured, e.g., in QALYs.
- Cost-consequence analysis: a form of cost-effectiveness analysis that presents costs and outcomes in discrete categories, without aggregating or weighting them.
- Cost-benefit analysis (CBA): compares costs and benefits, both of which are quantified in common monetary units.

Before a company or an organization decides on exactly which IDS that organization or company should opt, it is very important to perform cost/ benefit analysis. As it is very obvious and important that cost/benefit analysis is very real and important factor in decision making of all the process related to an organization. There funds allocated to the security or other solutions have to have a good reason why such funds are allocated to the said solution. This analysis can be performed effectively once the organizations risk analysis has been performed. This risk analysis will give the organization a very real sense of the costs associated company assets. The estimated cost/ benefit of the company can be evaluated with the following formulas as shown under:

$$\begin{aligned}\mathrm{Cost} = {} & \mathrm{Basic\ Cost\ of\ IDS(if\ any)} \\ & + \sum_{i=1}^{n} \mathrm{Deployment\ Cost} \\ & + \sum_{i=1}^{n} \mathrm{cost\ of\ Upgradation} \\ & + \sum_{i=1}^{n} \mathrm{Mointoring\ Cost}\end{aligned}$$

$$\text{where n is the number of assets}$$

The equation of cost has been designed to evaluate the total cost of the security solution for an organization. The cost consists of all the man power which can be used to incorporate the security solution in accordance to the requirement of the organization for the purpose of securing the critical data. Also the benefit is as important as determine the cost of security solution. The benefit will give us figures that whether the solution will be beneficial to the company. It will give us the impact of the benefits using the big budget for the security solution. The formula helps us to estimate the benefits from the security solution, which is usually the cost of assets which are currently under threat and future assets. The formulas for benefits are as under:

$$\begin{aligned}&\mathrm{Benefits} \\ &= \sum_{i=1}^{n} \mathrm{CostAssetsbenifitedbySecuritySolution} \\ &+ \mathrm{FutureAssetsbeniftedbySecuritySolution}\end{aligned}$$

$$\text{Where n is the number of Assets}$$

The Net Cost-Benefit will be retrieved from the difference of cost from benefits. The Net-cost benefit analysis will be derived as under:

$$\begin{aligned}&\mathrm{NetCost - BenefitsAnalysis} \\ &= \mathrm{Benefits - Cost}\end{aligned}$$

This section will be critical as far as the decision will be is concerned. If partially accepted from last sections, if the Net-Cost Benefits is greater than Zero (>0), it is again partially accepted.

3.6 Decision Phase

This is one of the most important phases of our framework, if the system is already partially accepted; it will go to the next

phase of detection. The final selection results will be based on the following points:

Name of IDS	Benefits
Snort	62,00,000
Bro	62,00,000
NIDS	62,00,000

1. Highest rate of detection under consideration.
2. Lowest False alarm Rate.
3. Highest Net-Cost Benefit.

It is considered that if the one security solution has high Net Cost-Benefits rate and rest two options are low and other solution have also been partially accepted but does not have Net Cost-Benefits but have very good statistics high in detection rate and true positive rate, the security solutions which have high detection rate and true positive rate will be considered for selection.

4.0 EVALUATION OF FRAMEWORK FOR CHOOSING INTRUSION DETECTION SYSTEM

The evaluation of frame work for choosing Intrusion detection system was done on the statistics provided by the Kashmir university IT&SS department. The department provided the statistics only meant for the research meant in this thesis. The figures provided are as :

Risk Analysis: As per the departmental report, total cost of assets which are under risk (attacks). The risk figures are calculated by using the above mentioned formulas.

$$\textbf{Risk} = \sum_{i=1}^{n} \textbf{No. of Assets} * \textbf{Cost}$$

Risk = Cost of Results + Cost of pay generation Software + Cost of E-Governance

Risk = 10,00,000 + 2,00,000 + 50,00000

Risk = 62,00,000 (Approx).

Pick IDS: We have chosen three intrusion detection systems which are open source. The selection of intrusion detection is based on statistics and popularity score in literature available. The intrusion detection systems are:

1. Snort.
2. Bro
3. NIDS.

Detection Rate: As per the literature available, we have collected the detection rate of the all the three intrusion detection system available. The detection rate is as under:

Name of IDS	Cost
Snort	1,30,000
Bro	1,50,000
NIDS	1,70,000

Table1: Detection Rate for evaluation

Name of IDS	Detection Rate
Snort	98.3 %
Bro	94.4 %
NIDS	97.3%

As per the statistics available in the literature, Snort has highest detection rate while on the second number NIDS is there and Bro is at the third number.

False Rate: As per the literature available, we have collected the respective false rate of the all the three intrusion detection system available mentioned above. The False rate is as under:

Table 2: False alarm Rate for evaluation

Name of IDS	False Rate
Snort	2.3%
Bro	7.5%
NIDS	2.1%

As per the statistics available in the literature, NIDS have least false rate, on second number Snort is there and last is Bro.

Cost-Benefit:

The benefit of all the three is as follows:

Table3: Cost Benefit for evaluation

The costs of all the three are:

Cost of Snort = Cost of Deployment + Cost of updating + Cost Maintenance.

Cost of Snort = 1, 00,000 (purchasing of Computer) + 0 + 30,000(rule purchasing)

= 1, 30,000.

Cost of Bro = Cost of Deployment
+ Cost of updating
+ Cost Maintenance (Script writing).

Cost of Bro = 1, 00,000(purchasing of Computer) + 10,000 per Month+ 40000(Script Writing)

= 1, 50,000.

Cost of NIDS= Cost of Deployment + Cost of Updating + Cost of Maintenance

Cost of NIDS = 1, 00,000(purchasing of Computer) + 50,000 per Month + 20,000

Cost of NIDS = 1, 70,000

Table 4: Cost for evaluation

Table5: Net Cost Benefit for evaluation

Net Cost-Benefit = Benefit – Cost

Name of IDS	Net Cost-Benefit
Snort	62,00,000-1,30,000 = 6070000
Bro	62,00,000- 1,50,000 = 6050000
NIDS	62,00,000 -1,70,000 = 6030000

Decision:
As the Net Cost-Benefit analysis for all are almost same, therefore the deciding factor is now detection rate and false alarm rate. As per the calculation Snort has highest detection rate from the three and rate of false alarm rate for snort is 2.3 and NIDS is 2.1. Therefore after seeing the results, the detection rate of Snort is high and false rate is almost same in NIDS and Snort, so we choose **Snort** from all the three intrusion detection system.

4.0 CONCLUSION

The current research is focused on choosing intrusion detection and prevention system. The selection of the Intrusion detection System is a very tough job. The thesis chapter provide framework for choosing best intrusion detection system for an organization. The framework is the form of flow diagram, when followed strictly will yield a solution for choosing best intrusion detection and prevention system for an organization. The steps mentioned in framework appears to be a simple exercise but are basically important/ critical steps for getting best of ID&PS for an organization . But ultimately the choice depends upon company. The researcher had made an attempt to provide certain guidelines in terms of frame work for choosing or selecting right most intrusion detection for an organization.

5.0 ACKNOWLEDGEMENT

I would like to thank Prof. S. M. K. Quadri, Head, Department of Computer Sciences, University of Kashmir for helping me throughout the course- Thank you Sir

6.0 REFERENCES

[1]. CONNOLLY, P. J., 2001. Security protects bottom line. InfoWorld, Vol. 23, No. 15, p. 47
[2]. SAKURAI, K., & Kim, T. H. (2008). A Trend in IDS researches. (Journal of Security Engineering), 5(4), 8.
[3]. Lazarevic, A., Ertoz, L., Kumar, V., Ozgur, A., & Srivastava, J. (2003). A comparative study of anomaly detection schemes in network intrusion detection. Proc. SIAM.
[4]. Mathew, D. (2002). Choosing an intrusion detection system that best suits your organization. GSEC Practical v1. 4b, available at: www. Sans. org/reading_room/whitepapers/detection
[5]. Brown, D. J., Suckow, B., & Wang, T. (2002). A survey of intrusion detection systems. Department of Computer Science, University of California, San Diego.
[6]. Grandison, T., &Terzi, E. (2009). Intrusion Detection Technology.
[7]. Beigh, B. M., & Peer, M. A. (2011). Intrusion Detection and Prevention System: Classification and Quick.
[8]. Kovacich, G. L. (2003). The Information Systems Security Officer's Guide: Establishing and managing an information protection program. Butterworth-Heinemann.
[9]. Huang, Y. A., & Lee, W. (2003, October). A cooperative intrusion detection system for ad hoc networks. In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (pp. 135-147). ACM.
[10]. Cavusoglu, H., Mishra, B., &Raghunathan, S. (2004). A model for evaluating IT security investments. Communications of the ACM, 47(7), 87-92.
[11]. Banerjee, U., & Arya, K. V. (2013). Optimizing Operating Cost of an Intrusion Detection System. International Journal of Communications, Network and System Sciences, 6(1).
[12]. Cohen, G., Meiseles, M., &Reshef, E. (2012). U.S. Patent No. 8,099,760. Washington, DC: U.S. Patent and Trademark Office
[13]. Amoroso, E., &Kwapniewski, R. (1998, December). A selection criteria for intrusion detection systems. In Computer Security Applications Conference, 1998. Proceedings. 14th Annual (pp. 280-288). IEEE.
[14]. Chaudhary, A., V. N. Tiwari, and A. Kumar. "Analysis of fuzzy logic based intrusion detection systems in mobile adhoc networks." BIJIT – BVICAM's International Journal of Information Technology, 6.1 (2014): 690-696.
[15]. Beigh, Bilal Maqbool. "One-stop: A novel hybrid model for intrusion detection system." INDIACom - 2014, 2014 IEEE International Conference on Computing for Sustainable Global Development, Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM). New Delhi, 2014.
[16]. Mitra, Sulata, and Arkadeep Goswami. "Load Balancing in Integrated MANET, WLAN and Cellular Network." BIJIT – BVICAM's International Journal of Information Technology, (2011): 304.