Network Intrusion Detection Systems based on Neural Network: A Comparative Study

Berlin H. Lekagning Djionang
University of Yaoundé I, Faculty of Sciences,
Yaoundé, Cameroon

Gilbert Tindo, PhD
University of Yaoundé I, Faculty of Sciences,
Yaoundé, Cameroon

ABSTRACT

Neural networks are artificial learning systems. For more than two decades, they have help for detecting hostile behaviors in a computer system. This review describes those systems and theirs limits. It defines and gives neural networks characteristics. It also itemizes neural networks which are used in intrusion detection systems. The state of the art on IDS made from neural networks is reviewed. In this paper, we also make a taxonomy and a comparison of neural networks intrusion detection systems. We end this review with a set of remarks and future works that can be done in order to improve the systems that have been presented. This work is the result of a meticulous scan of the literature.

Keywords

Intrusion detecting system, NIDS, neural network, MLP

1. INTRODUCTION

Intrusion detection systems are part of anti-intrusion systems. They consist on identifying and finding out suspicious or abnormal behavior within a computer system or network. Intrusion detection systems thus aim to protect computer systems and networks from attacks. An intrusion can be seen as the gap between what is defined in the security policy and the result of the intrusion detection system's analysis. During many decades, researchers have been working on building reliable and relevant IDS. Numerous methods have been used to achieve that goal. There are commonly three information sources that IDS can handle: log files, applicative logs and network packets. The latter is the target of our researches. Network services are most often subject to covetousness, what exposes the network to possible attacks. IDS are tools that detect attacks which cannot be detected at other security levels such as that of the firewall. One of the methods to implement intrusion detection systems is the neural network model. Many authors have suggested network detection systems based on neural networks. The success of neural networks come from the fact that they are able to learn a number of behaviors depending on network's input. In this work, we will dwell on neural network intrusion detection systems.

This review analyses the applicability of neural networks in intrusion detection within a computer network. Our work is organized as follows: first of all, we show the advantages and weaknesses of the approaches used in IDS. Secondly, we present the features of an artificial neural network. Thirdly, we analyze some works of researchers who explored neural networks intrusion detection systems. Then, we suggest a neural network-based taxonomy of IDS and finally, we highlight perspectives for future researches.

2. INTRUSION DETECTION SYSTEMS

In 1980, J. P. Anderson [1] introduced concepts and intrusion detection basis. He proposed some classification criteria [2]: detection model, post detection behavior, data sources from the events observed. There are three data analysis models: detection based on anomaly or behavior, detection based on misuse or scenarios and detection using specifications.

2.1 Scenario approach

All what is considered as normal is not hostile. It is imperative to know possible attacks, and keep in mind the following watchword [2]: "If it is not dangerous, then it is normal". Detection then consists on asking the following question: is the user's behavior a known intrusion?"

2.2 Behavioral Approach

This approach considers as abnormal everything that is not normal. A normal behavioris defined in opposition to every deviance which is considered as an attack. Its watchword [2] is: "If it is not normal, then it is dangerous." This approach consists of two steps: extracting information on the milieu in order to define the normal profile, putting in place of the boundaries beyond which the behavior is considered as normal. Detection has to do with asking the following question: is the present user's behavior congruent with previous behavior?

2.3 Specification Approach

This method builds the normal profile without using learning algorithms. The normal profile is defined through a specification of application's behavior or by defining a security policy [3]. The main disadvantage of this approach is that it requires many efforts during the putting in place of specifications; for each application to be watched [4].The advantages and disadvantages of the previous approaches are summarized in **Table n° 1.**

Table 1: **Advantages and Disadvantages of Intrusion Detection Approaches**

Approach / Evaluation	Advantages	Disadvantages
Scenarios	✓ Simplicity of implementation ✓ Fastness of diagnosis ✓ Precision (in view of the rules) ✓ Identification of the procedure of attack (procedure, target, source, tool)	✓ Only detects attacks known by the signature database ✓ Updates of the database ✓ Possible evasive techniques when the attacks are known
Behavioral	✓ Enables detection in principle of known attacks ✓ Facilitates the creation of rules adapted to these attacks ✓ Difficult to cheat	✓ False positive are relatively numerous ✓ Profile generation a is complex ✓ Need of a dataset geared ✓ Towards learning

3. NEURAL NETWORKS

3.1 Presentation of the concept

Neural networks are artificial learning methods. They are made of many neurons, placed in a network and organized in layers. Modelling a neural network is to describe the neural model and the connections between different neurons. A neural network can be partially connected, completely connected or organized in layers. The perceptron is the first operational model that recognized a configuration previously learnt. A formal neuron is the basic processing unit [5].

3.2 Why neural networks?

Neural networks are networks that are highly connected, with elementary processors which function in parallel and which are linked to each other by weights. These connection weights govern the functioning of the network. Each elementary process calculates a single entry on the basis of information it receives. Neural networks have several advantages in the implementation of intrusion detection systems. They are very effective and fast in classification [6]. They can easily identify new threats. Neural networks are able to process incomplete and imprecise data from multiple sources. The natural fastness of neural networks helps to reduce damages when the threat is detected [6]. The use of neural networks helps to extract non-linear relations existing between various packet fields and permits detect complex attacks in real time.

After having learnt correctly, neural networks have a good capacity of generalization; that means they are able to calculate with precision the corresponding output even if input data change. To enhance this generalization capacity, data have to be chosen so that they will be representative of the field being studied [5].The flexibility of neural networks is also one of the assets of intrusion detection [7].

4. NETWORK VULNERABILITIES

Network vulnerabilities are classified in four categories [8]: DOS, U2R, U2L and PROBES. These categories and attacks are described in **Table n°2**of the Appendix.

- DOS (Denial of service attacks): they aim to threaten services' availability by saturating computer resources and servers of targeted networks. These attacks achieved in networks have as direct consequences the freezing of the network traffic.
- Probes: attacks that aim to gather diverse information on the target, which can help an attacker to start on attack. There exists many types of probe attacks: some abuse rightful users and others use the engineering scheme to gather private information.
- R2L (Remote To Local): this attack aim to bypass or usurp authentication credentials of a target in order to execute some commands. Most of these attacks derive from social engineering [17].
- U2R (User To Root): Here, the attacks come from inside. The attacker usurps the administrator's password and thus the others users' credentials and data. Most of these attacks derive from the saturation of buffer caused by programming errors [17].

5. LEARNING METHODS USED IN NEURAL NETWORK-BASED NIDS

There are various models of NIDS based on neural networks:

✓ **Self-organizing maps (SOMs) :**

They are non-supervised methods of classification in which classes are discovered automatically. They are based on competitive learning. They are a visual method created by Kohonen which allow to reduce the size of the input vector. As a result, it produces two cards of one or two sizes representing inputs. It is a scheme for extracting knowledge.

✓ **Back propagation networks (BPN)** :

The algorithm of back propagation of mistakes is one of the methods which contributed to the development of neural networks. A back propagation of mistakes network is made of one input layer, one or two hidden layers and one output layer. The BPN can be used for classifying events such as attacks or normal traffic. One of their advantages is their generalization capacity and their natural ability of giving good approximations [6]. They are essentially used in prediction tasks they and facilitates supervised learning.

- ✓ **Radial Basic Function (RBF) network**:
RBF and MLPs are non-linear back propagation networks. They also give good approximations. The key difference between the two models is that a RBF model has one single hidden layer whereas the multi-layer perceptron has at least one hidden layer. The hidden layer's function of a RBF network is a non-linear function and its output is linear whereas the output of the multi-layer perceptron is non-linear.

6. RELATED WORKSON NEURAL NETWORK-BASEDIDS

Debar & all [9] is the first to use a neural network model to detect intrusions. The natural fastness of neural networks in detecting and recognizing attacks has influenced many researchers [7] [10], [11],[12], [13], [14], [15],[16] so as to make them get interested in this universal scheme for intrusion detection. The learning processes used for modifying the network's settings used by the researchers are the following:

- ✓ Present the data to the neural network in the form of a vector
- ✓ Make sure the generated output matches the desired one
- ✓ Change the network settings in order to match the desired output

In [10], James Cannady proposed an intrusion detection system based on the analysis of neural network protocols. In order to achieve the learning objective, he suggested three levels for preprocessing the packets:

- ✓ The first level of preprocessing deals with selecting relevant fields of a packet. The fields selected are the following: protocol ID-the following values are mapped to the protocols: TCP=0, UDP=1, ICMP=2 and Unknown =3; the source port number; the destination port number; the IP source address; the IP destination address; the ICMP TYPE- ICMP packet TYPE (Echo Request or Null), the size of the data in the packet and the shape of the data in the packet. It selects nine fields and some others that are not digital such as the ICMP TYPE.
- ✓ The second level deals with digitalizing non-digital data.
- ✓ The third level of preprocessing consists in changing those data into ASCII formats separated by commas and easy to handle by the neural network model. It uses the (MLP) multi-layer perceptron for learning. Our experiments demonstrated the ability of neural networks to detect different types of attacks in a network.

ALAN BIVENS & all [11] enhanced the system proposed by Canady. They noticed that Canady's system only detects attacks affecting the packet level. In their model, they attempted to generalize input data. Their method allows to detect attacks from multiple sources. They also associate the (MLP) neural network with Self-Organizing Map (SOMs) for detecting anomalies. SOM allows the organization of similar inputs while the MLP helps to determine which entry constitutes an attack. The number of clusters is constant and is determined during the learning step. The end process on the whole of the BDD99 dataset generates 76 % of false positive and 24 % of normal detection. Through their work, they showed that intrusion detection based on neural networks is possible with the use of supervised and non-supervised learning.

Mehdi MORADI and Mohammed ZULKERNINE [12] were the first to explore detection systems which detect not only attacks but also attack types. They used networks made of two or three layers. One the shortcomings with their model is overlearning, that is the inability of the network to detect new attacks. It is a problem that has to do with the generalization of the network. They notice that detection with a three-layer network is more reliable than a two-layer one. The main weakness here is the number of attack types that their model can detect. Certain authors lifted that limitation and went further beyond.

Vladimir Golovko and Pavel Kochuko [7] suggest an intrusion detection system based on the analysis of network traffics. The detection system they propose consists of several levels. It collects network packets by means of a sniffer located on WinPCap, UNIX pcap and send them to a preprocessing module. The work of this last module consists in selecting the data to be transmitted to the neural network. It gathers the data of the IP, TCP, UDP, and ICMP protocols. The system analyses the heading of packets and calculates the settings of TCP connections. Those settings are the following: the duration representing the number of seconds of the connection, the type of protocol (tcp, udp …), the destination service (http, telnet ….), the number of bytes which travels from the source to the destination, the number of bytes which travels from the destination to the source, a destination parameter which stands at 1 when the authentification goes smoothly and stands at 0 if not and a TCP/IP.

This system permits the detection and recognition of new attacks. The MLP architecture it uses is made up of 6 entries, 40 hidden neurons and 60 exits. The experiment including the KDD99 data set permits to say the system is effective for a certain kind of attacks: 99.98 % detection for attacks of the dos type (this attack aims at saturating the network and making it unavailable), 94.62 % of recognition, 3.84 % for detection of attacks of the u2r type (unauthorized access to the privilege of the super user) and 0 % for recognition, 45.2 % for detection of attacks of the r21 type (unauthorized access to a remote device), 97. 64 % for recognition, 98.78 % for detection of attacks of the type probe (scans and gets confidential data) and 79.86 % for recognition.

To enhance the previous system VAITSEKHOVICH and GOLOVKO [13] suggested several architectures based on the MLPs and LPCA (Linear PCA (principal component analysis) neural network). The PCA network is used to extract data and reduce the size of the data vector. The multi-layer perceptron (MLP) is used for detecting and recognizing attacks. In the first architecture, VAITSEKHOVICH and GOLOVKO proposed to directly connect the PCA to the MLP. The PCA consists of 41 entries and 12 exits. The second architecture which is made of 4 MLP networks deals with detecting one of the four categories of attacks (Dos, U2R, R2L and Probe). The exits of these multi-layer networks are connected to an arbiter which takes the final decision as regards the etching class. The learning of the arbiter is effective after the learning of the LPCA and the learning of the MLPs. The last architecture derives its inspiration from the divide and reignrule used in solving complex problems. Kit consists on submitting the 414 entries to three experts. But the learning algorithms of these experts are not identical. And here an expert represents a simple classification system and the first architecture we will describe. The entries of experts are also associated with an arbiter as with the previous architecture.

Also called RNN (recircular neural network), the PCA is a multi-layer perceptron consisting of de 41 entries, 12 hidden layers and 41 exits. It has been noticed that the hidden layer can stand as a bottleneck during the learning step. This is rather an asset because it allows the compression of input data to be better in performances.

The KDD data are therefore used for learning and testing various architectures that are suggested. The model three permits to correctly detect attacks but the difference relies in the rate of false positives, whichis closed to 48 % and 14% for the first two models and 13% for the latter model. We can concludes that the latter model is better than the two others.

Aslihan Ozkaya && Bekir Karlik [14] have suggested an intrusion detection system of the protocol type based on RBF neural networks after preprocessing the whole KDD99 dataset. This preprocessing step affects non-digital fields. They are carrying out three types of normalization on those fields and it turns out that matching numbers to non-digital fields on the basis of their frequency of appearance is not the right solution. According to this work, the best solution shows that random values have to be attributed to non-digital fields in order to better performance of the neural network-based IDS. The detection rate obtained after affecting that preprocessing stands at 93.42 %with an average false positive rate of 2.95%.

Muna Mhammad & Monica Mehrotra [15] suggested an IDS based on a hybrid model for detecting not only attacks but also categories of attacks. The algorithm of clustering Fuzzy C-Means is used to classify attacks and non-attacks whereas the neural model is used for identifying attack types. This classification algorithm brings about a classification rate of 99.99 % and a false positive rate of 0.01%. They compared various activation functions for learning and reached the conclusion that the sigmoid function is better than the other functions. The recognition rate of the attack types stands at 78 % while the recognition rate of new attacks is 82%.

Yousef Abuadlla && all [16] suggested a behavioral IDS based on traffic networks and two levels of neural networks. The first level makes possible the changes within the traffic and checks whether it is an attack or not. If the former is true, the second level of the neural network determines which type of attack it is. Two neural networks models are used: the MLP and RBF models. The system they suggested is made of five modules: a module for collecting data flow, one for preprocessing, one for detecting anomalies, one for detecting types of attacks and a warning module. The detection rate obtained is 99.4%, and 0.3 % of false positive as regards the model designed with the MLP. This rate stands at 95.4% for recognition and 2.6 % of false positive for the RBF model. The recognition rate for new attacks is 78%.

[17] Propose a deep learning based approach for developing such an efficient and flexible NIDS.

7. TAXONOMY OF NEURAL NETWORK-BASED IDS

The IDS taxonomy that we suggest is represented in **Figure 1.** This taxonomy permits to bring out the various models used at each level of a NIDS. The **optional level 1** is used for detecting normal and abnormal packets while the last level, which is compulsory effectively, permits to detect attack type or category.

8. COMPARATIVE STUDY

In this section, we are carrying out a comparative study of neural network-based IDS. [15] Started this work by presenting a comparative table containing the results. **Table n°3**summarizes the works of authors who have come up with quantitative results. All these works are based on the KDD99 dataset or its derivatives.

Table n°3:Summary of the results of the works on NR-based IDS

Author criteria	Classification rate	False Positive	False negative
Mehdi 2004	87%	-	-
Srinivas 2005 [18]	97,07%	0,20%	2,7%
Dima 2006	93%	0,8%	-
Iftikar 2008 [19]	95,93%	-	-
Pizeniyslaw 2008	92%	8,8%	-
Khattab 2009[21]	97%	2,4%	0,8%
Muna 2010	99,9%	0,01%	0,01%
Vaitsekhovich 2008	93,21%	12,90%	-
Golovko 2005	94,3%	-	-
Aslihan 2012	93,42%	2,95%	-
Yousef 2012	99,4%	0,3%	-
Yousef 2012	95,4%	2,6%	-
Iftikar 2009 [20]	98%	1,5%	-
Alan 2002	24%	76%	-

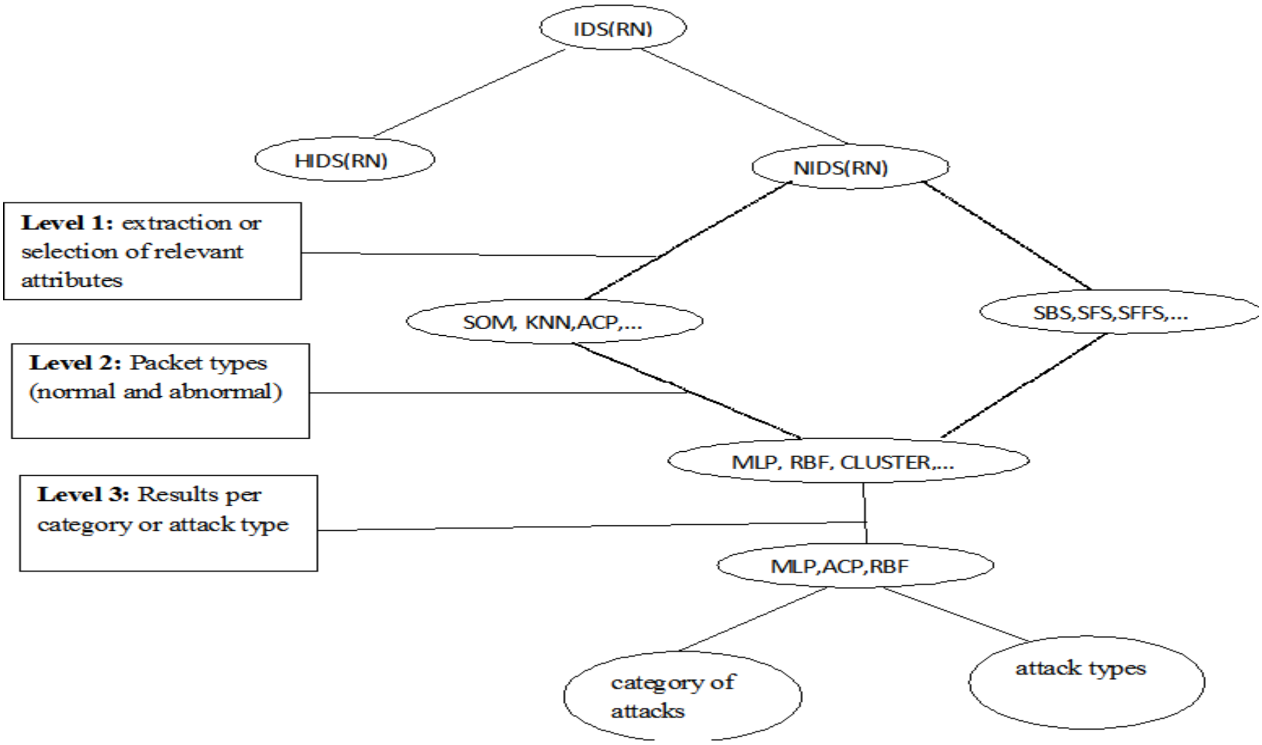
IDS(RN)
HIDS(RN)
NIDS(RN)
Level 1: extraction or selection of relevant attributes
SOM, KNN,ACP,...
SBS,SFS,SFFS,...
Level 2: Packet types (normal and abnormal)
MLP, RBF, CLUSTER,...
Level 3: Results per category or attack type
MLP,ACP,RBF
category of attacks
attack types

Figure2: **Taxonomy of IDS**

9. CONCLUSION AND PERSPECTIVES

The current work had to do with giving an overall presentation of the concepts of IDS, neural networks and its importance for the designing of IDS. We have studied the works related to neural network-based NIDS, done an overall and recapitulative assessment and setup a taxonomy of categories of IDS. We noticed that several authors have suggested reliable and relevant IDS. It should be noted that an important work has to be done at the level of selecting and extracting knowledge, for the IDS which highlighted **Level 1** has a good classification rate. The selection and extraction of relevant attributes can help to boost the performance of IDS. Most of these works present the NIDS which are not flexible because a single model of neural networks allows to detect the categories of attack. The future works can dwell on the flexible architectures to better the performances of the IDS. It will be also interesting to find a model of characterization of normal packets and attack types.

10. REFERENCE

[1] J.P. A NDERSON. “Computer Security Threat Monitoring and Surveillance”. Rapport Technique, James P. Anderson Company, Fort Washington, Pennsylvania, April 1980.

[2] Ludovic Me, « Méthodes et outils de la détection d’intrusions », Supelec.

[3] Guillaume Hiet, « Détection d’instructions paramétrée par la politique de sécurité grâce au contrôle collaboratif des flux d’informations au sein du système d’exploitation et des applications: mise en œuvre sous linux pour les programmes java » Université de Rennes, Decembre 2008

[4] Asmaa Shaker, Sharer Gore « Importance of Intrusion Detection System » International Journal of Scientific & Engineering Research Janvier 2011.

[5] Nicoleta Minoiu « comparaison entre l’analyse logic et probit et les réseaux de neurones »

[6] G. DREYFUS “les réseaux de neurones” Mécanique Industriel et Matériaux, n51, septembre 1998

[7] Vladimir Golovko, Pavel Kochurko “Intruision recognition using neural networks” International Scientific Journal of computing, 2005, vol. 4, Issue3, 37-42

[8] Mahbod Tavallaee && all “A Detailed Analysis of the KDD CUP 99 Data Set” Proceeding of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Application (CISDA 2009)

[9] H. Debar && all, “A neural network component for an intrusion detection system”, in IEEE Symposium on Research in Computer Security and Privacy, Oakland, 4– 6 May 1992 (IEEE, Amsterdam, 1992), pp. 240– 250

[10] James Canady “Artificial Neural Networks forMisuse Detection,” Proceedings, National Information Systems Security Conference (NISSC), 98

[11] ALAN BIVENS && all “Network based intrusion detection using neural network” Intelligent Engineering Systems through Artificial Neural network ANNIE-2002, St. Louis,MO,vol. 12, ASME Press, New York,NY, 2002, pp. 579-584

[12] Mehdi MORADI and Mohammad ZULKERNINE, “A Neural Network based System for intrusion detection and Classification of Attacks” In 2004 IEEE International on Advances in Intelligent Systems.

[13] Leanid VAITSEKHOVICH, Vladimir GOLOVKO « Employment of neural network baser classifier for intrusion detection » acta mechanica et automatica, vol2, no4, 2008

[14] Aslihan Ozkaya && Bekir Karlik "Protocole Type Based Intrusion Detection Using RBF Neural Network" International Journal of Artificial Intelligence and Expert Systems (IJAE), volume (3): Issue (4):2012

[15] Muna Mhammad && Monica Mehrotra "Design Network Intrusion Detection System using Hybrid Fuzzy-Neural Network" International Journal of Computer Science and Security, volume (4): Issue (3): 2012

[16] Yousef Abuadlla && all "Flow-Based Anomaly Intrusion Detection System Using Two Neural Network Stage", Computer Science and Information systems 11(2): 601-622: 2012

[17] Quamar && all "A Deep Learning Approach for Network Intrusion Detection System" BICT 15 Proceeding of 9th EAI International Conférence on Bio-inspired Information and Communications Technologies (BIONETICS) pages 21-26, December 2015

[18] Srinivas Mukkamala && all "Intrusion detection using an ensemble of intelligent paradigms", Journal Network and Computer Applications 28 (2005), 167-182

[19] Iftikhar Ahmad && all "Performance Comparison between Backpropagation Algorithms Apllied to Intrusion Detection in Computer Network Systems" WSEAS International Conference on NEURAL NETWORKS, Sofia, Bulgaria, May 2-4, 2008

[20] Iftikhar Ahmad && all "Application of Artificial Neural Networmanyk in Detection of Probing Attacks" 2009 IEEE Symposium on Industrial Electronics and Applications(ISIEA 2009), October 4-6, 2009, Kuala Lumpur, Malaysia

[21] Khattab Ali && all "The Effect of Fuzzification on neural Networks Intrusion Detection system" IEEE computer society 2009

[22] Mohammad Khubeb Siddiqui and Shams Naahid "Analysis of KDD CUP 99 Dataset using Clustering based Data Mining", International Journal of Database

11. APPENDIX

The Attacks per Category of the NLS-KDD99 Data Set are Organized in Terms of Training and Testing Data.

Table n°2 : Attack Types

Category	Attack types	Training	Test	Category	Attack types	Training	Test
Normal	Normal	67 343	9711	DOS	neptune	41214	4657
R2L	ftp_write	8	3		pod	201	41
	guess_passwd	53	1231		processtable	0	685
	httptunnel	0	133		smurf	2646	665
	imap	11	1		teardrop	892	12
	multihop	7	18		udpstorm	0	2
	named	0	17	U2R	buffer_overflow	30	20
	phf	4	2		loadmodule	9	2
	sendmail	0	14		perl	3	2
	snmpgetattack	0	178		ps	0	15
	snmpguess	0	331		rootkit	10	13
	warezmaster	20	944		sqlattack	0	2
	worm	0	2		xterm	0	13
	xlock	0	9				
	xsnoop	0	4				
Probes	ipsweep	3599	141				
	mscan	0	996				
	nmap	1493	13				
	portsweep	2931	157				
	saint	0	319				
	satan	3633	735				
DOS	apache2	0	734				
	back	956	359				
	land	18	7				
	mailbomb	0	293				