Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Application of Neural Networks to Intrusion Detection

Intrusion Detection Systems (IDS) are now mainly employed to secure company networks. Ideally, an IDS has the capacity to detect in real-time all (attempted) intrusions, and to execute work to stop the attack (for example, modifying firewall rules). We present in this paper a " state of the art " of Intrusion Detection Systems, developing commercial and research tools, and a new way to improve false-alarm detection using Neural Network approach. This approach is still in development, nevertheless it seems to be v...

Copyright SANS Institute
Author Retains Full Rights

AD

Jean-Philippe PLANQUART
GSEC Certification - version 1.2d

Application of Neural Networks to Intrusion Detection

Introduction

Intrusion Detection Systems (IDS) are now mainly employed to secure company networks. Ideally, an IDS has the capacity to detect in real-time all (attempted) intrusions, and to execute work to stop the attack (for example, modifying firewall rules). We present in this paper a « state of the art » of Intrusion Detection Systems, developing commercial and research tools, and a new way to improve false-alarm detection using Neural Network approach. This approach is still in development, nevertheless it seems to be very promising for the future.

This paper is organized as follows : first, we present the global architecture of IDS and a few commercially available tools, then we analyze new axes of research to improve IDS's performances and particularly the application of Neural Networks to Intrusion Detection.

Classification of Intrusion Detection Systems

A guidance document on Intrusion Detection Systems is available from National Institute of Standards and Technology (NIST) organization [1].

Intrusion Detection Systems can be classified into three categories :

- **host-based IDS**, evaluate information found on a single or multiple host systems, including contents of operating systems, system and application files.
- **network-based IDS**, evaluate information captured from network communications, analyzing the stream of packets traveling across the network. Packets are captured through a set of sensors.
- **vulnerability-assessment IDS**, detect vulnerabilities on internal networks and firewalls

There are two primary models to analyzing events to detect attacks:

- **misuse detection model** : IDS detect intrusions by looking for activity that corresponds to known signatures of intrusions or vulnerabilities
- **anomaly detection model** : IDS detect intrusions by searching « abnormal » network traffic

Most IDS commercial tools refer to the misuse detection model, and signatures of intrusions must always be updated by vendors.

IDS based on anomaly detection model have the ability to detect symptoms of attacks without specifying model of attacks, but they are very sensitive to false alarms.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Commercially available tools

A Jackson [2] of Los Alamos National Laboratory wrote a complete survey of IDS products. Characteristics for each of the seventeen products are studied according to nine major features :

- **suitability** for IDS architecture and management scheme
- **flexibility** of adaptation for a specific network to be monitored
- **protection** against malicious tampering
- **interoperability** with other network management and security tools
- **comprehensiveness**, to expand the concept of intrusion detection such as blocking Java applets or Active-X controls, monitoring e-mail content, blocking specific urls
- **event management**, such as managing and reporting event trace, updating attack database
- **active response** when an attack occurs, such as firewall or router reconfiguration
- **support** for product

Another recent market survey of commercially available Intrusion Detection tools today is available in [3]. We present here examples of IDS tools, classified according to the three models : host-based, network-based and vulnerability-assessment tools

Host-based IDS tools

Host-based IDS systems detect attacks for an individual system, using system logs and operating system audit trials. Examples of well known host-based commercial tools are : Cybercop from Network Associates (NAI) (http://www.pgp.com), KaneSecurity Monitor (KSM) from RSA Security (http://www.rsasecuriy.com). Tripwire (http://www.tripwire.org) is a specific tool to detect changes of administrative or user files on one server.

Network-based IDS tools

Network-based IDS systems detect attacks by capturing and analyzing network packets, from « sensors » placed at various points in a network. Examples of well known Network-based commercial tools are : RealSecure from Internet Security Scanner (ISS) (http://www.iss.net), Cisco Secure IDS or NetRanger from Cisco Systems (ex Wheel Group Corporation), Centrax from CyberSafe corporation, and Network Flight Recorder NFR

A popular and freely-available Network-based IDS is Snort, a lightweight IDS (http://www.snort.org)

The main difficulty for Network-based IDS is to process in real-time all packets for a large network ; specific hardware solutions may be employed. Another problem is segmentation of networks by switches which involve difficulties in capturing traffic for a global network.

Vulnerability-assessment tools

Vulnerability-assessment tools are security scanners used to detect known vulnerabilities on specific Operating System's configuration. Examples of well-known vulnerability-assessment tools are : CyberCop Scanner from PGP Security (a Network Associates Division) and SecureScan NX from Networks Vigilance (formally known as NV e-secure).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

A freely-available vulnerability-assessment tool is Nessus, a Linux-based vulnerability scanner (http://www.nessus.org) written by R. Deraison

Performances for commercial tools

The majority of tools available today refer to the misuse detection model, meaning that administrators need to regularly update vulnerabilities database. Then, all these tools are vulnerable to new signatures of attacks.

Tools are also very sensitive to false attacks, corresponding to normal network traffic.

Major commercial IDS do not handle Fragmentation / re-assembly of IP packets.

For large networks, it would be necessary to store Gigabytes of event data every day, to treat them off-line.

Application of Neural Networks to Intrusion Detection

The Center for Education and Research in Information Assurance and Security (CERIAS) has produced a review of IDS research prototypes [4], and a few are now commercial products.

Approaches for misuse detection

Approaches for the misuse detection model are :

- **expert systems**, containing a set of rules that describe attacks
- **signature verification**, where attack scenarios are translated into sequences of audit events
- **petri nets**, where known attacks are represented with graphical petri nets
- **sate-transition diagrams**, representing attacks with a set of goals and transitions

The common approach for misuse detection concerns « signature verification », where a system detects previously seen, known attacks by looking for an invariant signature left by these attacks. This signature is found in audit files, in host-intrused machine, or in sniffers looking for packets inside or outside of the attacked machine.
Limitation of this approach is due to :

- frequent false-alarm detection
- the need to specify a signature of the attack, and then to update signature of attacks on every IDS tool. A signature of an attack may not be easily discovered.
- new attack signatures are not automatically discovered without update of the IDS

Approaches for anomaly detection

Anomaly Detection in Network-based or Host-based IDS includes :
- **threshold detection** detecting abnormal activity on the server or network, for example abnormal consumption of the CPU for one server, or abnormal saturation of the network
- **statistical measures**, learned from historical values
- **rule-based measures,** with expert systems
- **non-linear algorithms** such as Neural Networks or Genetic algorithms

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The common approach for anomaly detection concerns the statistical analysis, where the user or the system behavior is measured by a number of variables over the time. These variables may be the login and the logout time of each session, the amount of resources consumed during the session, and the resource duration. The major limitation of this approach is to find a correct threshold without frequent false-alarm detection.

DARPA Intrusion Detection Data Base

To improve performances of IDS systems with real network traffic, a large-scale realistic Intrusion Detection data-base has been sponsored by the US Defense Advanced Research Projects Agency (DARPA) in 1998. More than two months of traffic observed from US Government sites and the Internet were registered, adding attacks against various hosts OS. DARPA data-base was then designed to evaluate performances of Intrusion Detection Systems. The first evaluation with off-line and real-time Data Base was conducted in the summer of 1998 [5].

Neural Network approach for Intrusion Detection

One promising research in Intrusion Detection concerns the application of the Neural Network techniques, for the misuse detection model and the anomaly detection model. Performance evaluations presented in this paper all refer to the DARPA Intrusion Data Base.

Neural Network approach

An artificial Neural Network consists of a collection of treatments to transform a set of inputs to a set of searched outputs, through a set of simple processing units, or nodes and connections between them. Subsets of the units are input nodes, output nodes, and nodes between input and output form hidden layers ; the connection between two units has some weight, used to determine how much one unit will affect the other. Two types of architecture of Neural Networks can be distinguished :

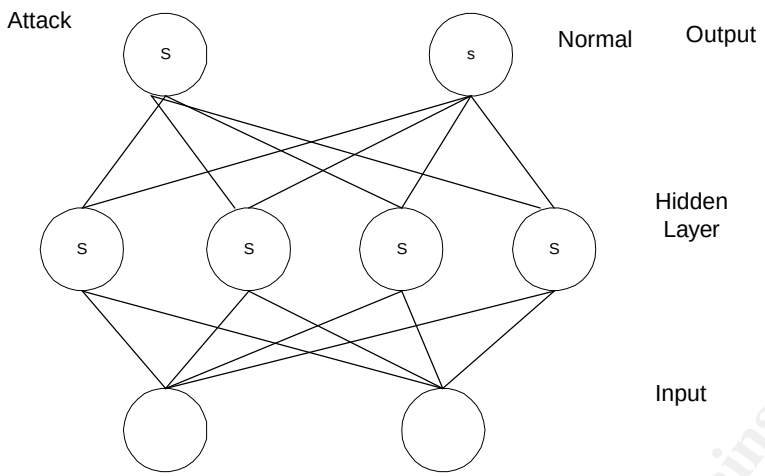
- **Supervised training algorithms**, where in the learning phase, the network learns the desired output for a given input or pattern. The well known architecture of supervised neural network is the Multi-Level Perceptron (MLP) ; the MLP is employed for Pattern Recognition problems.
- **Unsupervised training algorithms**, where in the learning phase, the network learns without specifying desired output. Self-Organizing Maps (SOM) are popular unsupervised training algorithms ; a SOM tries to find a topological mapping from the input space to clusters. SOM are employed for classification problems.

A good introduction to Neural Networks is available in [6]. The most important property of a Neural Network is to automatically learn / retrain coefficients in the Neural Network according to data inputs and data outputs. Applying the Neural Network (NN) approach to Intrusion Detection, we first have to expose NN to normal data and to attacks to automatically adjust coefficients of the NN during the training phase. Performance tests are then conducted with real network traffic and attacks.

Neural Networks have been largely employed with success for complex problems such as Pattern Recognition, hand-written character recognition, Statistical Analysis. We present four recent studies on the application of the Neural Network approach to the scope of Intrusion Detection, both for the misuse detection model and the anomaly detection model.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Representation of a Perceptron with one Hidden Layer (from [8])



Georgia University neural network IDS

J Cannady and J Mahaffey [7] of Georgia Technical Research Institute (GTRI) conducted research to apply Multi-Level Perceptron (MLP) model and MLP/SOM (Self-Organizing Maps) for misuse detection.

The MLP prototype had these characteristics : 4 fully connected layers, 9 input nodes and 2 output nodes (normal and attack). With this prototype, they simulated specific attacks as ISS scans, SATAN scans and SYNFlood, and each attack was clearly identified through normal traffic.
A MLP/SOM prototype was then designed to detect dispersed and possibly collaborative attacks. Neural Network was a feed-forward network with back-propagation learning. In the learning phase, Neural Network converged rapidly. Preliminary results with unsuccessful FTP login attempts where correctly identified as attacks.

MIT research in neural network IDS

R Lippmann and R Cunningham [8, 9] of the MIT Lincoln Laboratory also conducted tests applying Neural Networks to misuse detection model, by searching for attack-specific keywords in the network traffic. They used a Multi-Level Perceptron (MLP) to detect Unix-host attacks, and attacks to obtain root-privilege on a server. Generic keywords are selected to detect attack preparations and actions executed after.

A two-layer perceptron was designed with k input nodes, 2k hidden nodes and 2 outputs (normal and attack) ; backpropagation in the learning phase detects weights of the Neural Network. Good detection performance was obtained with 30 keywords to detect attacks, such as « cat > », « uudecode » or new root shell (« uid=0(root) », « bash# »).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Applied to Shell source code with 7 shell-commands representing an attack, 17 out of 20 attacks were detected and one false alarm generated ; applied to C source code with 2 features, 68 of 73 attacks were detected and 4 false alarms.

With the Neural Network approach, false alarms were reduced by two orders of magnitude (to roughly one false alarm per day) and they increased the detection rate to roughly 80 % with the DARPA data base. System could detect old as well as new attacks not included in the training data, and in a lesser extent attacks distributed across multiple sessions.

UBILAB Laboratory

Luc Girardin of the UBILAB laboratory [10, 11] also employed Self-Organizing Maps (SOM) to perform clustering of network traffic and detect attacks based upon Neural Network, associated with a visual approach of network traffic. SOM are employed to project network events on an appropriate 2D-space for visualization, and then they are displayed to the Network Administrator with a comprehensive view of traffic. Intrusions are then easily extracted from this view, by highlighting divergence from the norm with visual metaphors of network traffic.

Girardin tested this approach with success for the following attacks : IP spoofing, FTP password guessing, network scanning and network hopping ; log file systems are analyzed from firewalls. However, this approach needs a visual interpretation of network traffic by an administrator to detect attacks.

Research of RST Corporation

A Ghosh and A Schwartzbard [12] of Reliable Software Technologies Corp. used the Neural Network approach for the anomaly detection model by analyzing program behavior profiles for Intrusion Detection. Program behavior profiles are built by capturing system calls made by the program, to monitor the behavior of programs by noting irregularities in program behavior.

Their IDS was a single hidden layer Multi-Layer Perceptron (MLP) ; they also employed the so-called Lucky Bucket algorithm to keep in mind temporal memorization of recent abnormal events, by managing a counter : for a normal output, the counter tends to be zero, and for an anomaly the counter tends to be one.

Performance for their system was tested with the DARPA data-base, including intrusive and non-intrusive sessions. Applied to anomaly detection, system detects with good performances known and new attacks (77 % of attacks where detected with 3 % of false alarms), but application to misuse detection detects attacks with high false alarm rates, excluding usage for commercial use. In 1998, with the DARPA off-line IDS evaluation, the system successfully detected User-to-Root attacks composed of system-call sequences.

In order to improve the anomaly detection model, A Ghosh et al. [13] then tested Intrusion Detection to another topology of Neural Network, the Elman Network for recognizing recurrent features in program execution traces. An Elman Network is based on a feed-forward topology with the addition of context nodes retaining information from previous inputs. Applied to the DARPA database, the Elman Networks were able to detect 77 % of attacks with **no false alarm**, improving results obtained with the MLP topology.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

In 1999, during the evaluation of performance tests with other systems and applying the DARPA data-base, this system had promising results with anomaly detection to detect new attacks.

Conclusion

Intrusion Detection Systems are becoming largely employed as a fundamental Network Security system. Commercial tools available today have limitations in detecting real intrusions, and Neural Network is a efficient way to improve the performances of IDS systems which are based on the misuse detection model and the anomaly detection model.

© SANS Institute 2001, Author retains full rights.

References

[1] Bace R & Mell P - NIST Special publication on Intrusion Detection Systems (http://csrc.nist.gov/publications/drafts/idsdraft.pdf)

[2] Jackson A - Intrusion Detection System (IDS) product survey - Los Alamos National Laboratory - New Mexico (http://lib-www.lanl.gov/la-pubs/00416750.pdf)

[3] Infosecurity magazine July 2001 - available on-line at http://www.infosecnews.com

[4] Dacier M & A Wespi A - Towards a taxonomy of intrusion-detection systems H Debar, Computer Networks 31 (1999) 805-822

[5] DARPA Intrusion Detection Evaluation - MIT Lincoln Laboratory - (http://www.ll.mit.edu/IST/ideval)

[6] Anderson J - An introduction to Neural Networks - MIT Press 1995

[7] Cannady J & Mahaffey J - The application of Artificial Neural Networks to Misuse detection : initial results - Georgia Tech Research Institute (http://www.raid-symposium.org/raid98/Prog_RAID98/Talks.html#Cannady_34)

[8] Cunningham R & Lippmann R - Improving Intrusion Detection performance using Keyword selection and Neural Networks R - MIT Lincoln University (http://www.ll.mit.edu/IST/pubs.html)

[9] Cunningham R & Lippmann R - « Detecting Computer Attackers : recognizing patterns of malicious, stealthy behavior - MIT Lincoln Laboratory - Presentation to CERIAS 11/29/2000 (http://www.cerias.purdue.edu/secsem/abstracts0001.php)

[10] Girardin L. and Brodbeck D.- A Visual Approach for Monitoring Logs. In Proceedings of the 12th System Administration Conference (LISA '98), pages 299-308, Boston, MA, December 1998. (available at http://www.ubilab.org/publications/index.html)

[11] Girardin L - An eye on network intruder-administrator shootouts - UBS UBILAB In Proceedings of the 1st Workshop on Intrusion Detection and Network Monitoring (ID '99), Santa Clara, CA, (http://www.ubilab.org/publications/index.html)

[12] Ghosh A & Schwartzbard A - A study using Neural Networks for anomaly detection and misuse detection - Reliable Software Technologies - (http://www.docshow.net/ids/usenix_sec99.zip)

[13] Ghosh A, Schwartzbard A & Schatz A - Learning program behavior profiles for Intrusion Detection - Proceedings of the workshop on Intrusion Detection and Network Monitoring - Santa Clara, April 9-12 1999

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**