REPUBLIQUE ALGERIENNE DEMOCATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Centre de Recherche sur l'Information Scientifique et Technique
CE RIST

Mémoire

Pour l'obtention du Diplôme de
Post Graduations spécialisée en Sécurité Informatique

Thème

SYSTEME DE DETECTION D'INTRUSIONS

Présenté Par : Mr Morsli OUMRANI (CRNB)

Promoteur :Pr Ahmed NACER (USTHB)

CERIST. 2004

IF A FIREWALL IS YOUR FIRST PERIMETER THEN AN IDS MUST BE YOUR SECOND

INTRUSION DETECTION SYSTEMS

MORSLI Oumrani , June 2004, CERIST, ALGIERS.

Outlines

ACKNOWLEDGEMENTS

First and foremost, thanks to Allah and my parents.

To my major professor Dr. A.NACER ...to Mme BENMEZIANE and the the staff of CERIST.

Thanks to my wife , without her encouragement and help,I couldn't have completed this project.

Thanks to Mr KHELALFA , He taught me and put me on the IT security road.

ABSTRACT

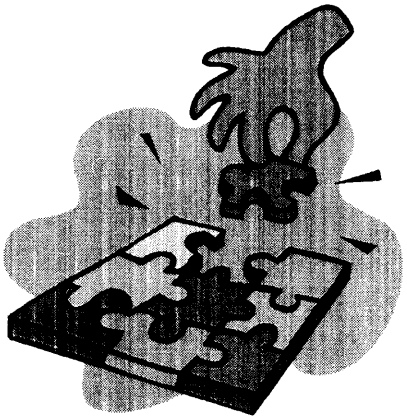
With the daily advancements in technology today, the rate at which intrusions take place is increasing .In 2001, the Code Red worm was released and replicated approximately every 37 minutes.
The Slammer worm, released in January 2003, had a doubling rate of 8.5 seconds...Others are coming.
Even an organization may invest time, money, and resources into setting up protective technologies such as firewalls, encryption, authentication, proxies, gateways, PKI, VPN, access control, virus detection/removal, etc...
The IDS serves in sitting back and watching if the above technologies are working .
That why IDS's are invented ,but as user what IDS to choose ......

PREFACE

The world now becomes more and more interconnected , administrative and commercial IT systems are dependant on availability, integrity and confidentiality of information that traverse these systems , thus a security model must be implemented ,this model must include beside a user-policy and firewalls a system called Intrusion detection systems . Intrusion Detection Systems are only one piece of the whole security puzzle ;they must be supplemented by other security and protection mechanisms ; They are a very important part of a security architecture but does not solve all problems

Intrusion detection permits an organisation to identify unusual activities occurring on information traffic ,Intrusion detection systems can generate real-time email or pager warning to predefined system administrators ,an alarm to system management consoles or log an alerts to a file or a database, IDS response may also include initiation of a predefined action to block or impose rate restrictions on a offending attack.

Commercial IDS presents an evolving market ,considerable changes in their technical architecture is taking into account , integration of network infrastructure ,routers, switches.., consolidation with other applications and security tools (1),correlation of security events as standard meaning ,tuning features ,overcoming speed processing and bandwidth problems.



INTRODUCTION

IDS work falls in one of the three axes :Product Survey, Detection techniques, Benchmarking and evaluation , this project gives a summary on the history and evolution of intrusion detection analysis and actual players in this domain like cisco ,iss , symantec , networkice ,interasys and others. Then the architecture of a system by emphasizing on the unit that is responsible for detection and analysis , the user is sensed to know what technique is used in his future application on analyzing the data.

A view is given in benchmarking efforts done in many labs and by many groups to get an effective methodology in testing and evaluating a product as well as standardizing terminology and maintaining a minimum of interoperability between existing IDS players.

Well choosing an appropriate application for intrusion detection is the goal behind this work , a list of criteria and questions must be asked by any one in the way of acquiring a product.

Snort as an open source IDS is choosed as prototype , the big fiches like ISS and cisco use it as reference because of its multifunction capabilities and scalability as well as its rich attack signature database.

Although much academic and commercial work has been done to evaluate the quality of IDS, choosing adequate intrusion detection solution remains a difficult decision-making ,not only a good knowledge of network intrusion detection principles is a must but also networking, various operating systems, exploit and vulnerability news and other area in security for classifying existing products and making choice decision .

Definition

We can think of an intrusion detection system as an alarm system. The alarm does not provide the security itself; the security is achieved through the use of locks and other controls. The alarm is a means to indicate that *some sort of potentially malicious activity is being attempted.*

Unlike the anti-virus industry, where products have approximately similar signature capabilities intrusion detection vendors have different approaches, and techniques.

IDS products identify security policy violations by applying one of the two methodologies .

A signature based or anomaly based analysis . The first identifies an intrusion by its signature or a pattern database of known security exploits ,for example an IDS could interrogate network traffic to find a simple text string as "phf" as indicator of an attempt to exploit a vulnerable CGI program .

The second method used by IDS vendors to perform intrusion detection systems using anomaly detection routines where abnormal network traffic could be defined as traffic that does not behave to a protocol RFC or falls outside of the bounds of **Normal (2)**traffic characteristics or volume.

Organizations should also consider constraints imposed by their network topology ,hardware and software infrastructure:

- Network topologies—Ethernet, T1/E1, etc.
- Operating systems—specific Unix OS , MS Windows, Novell NetWare, etc.
- Switched networks.
- Protocols—ICMP, IP v4, IP v6, TCP, UDP, etc.
- Applications—FTP, HTTP, Secure Shell (SSH), Telnet, etc.

perform intrusion detection as part of firewall and intrusion detection should be a *function* and not a