International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 4, Issue 5 (October 2014) PP: 28-41

Honey Pot Intrusion Detection System

[1]Kwama Leonard Ogweno, [2]Obare Erick Oteyo, [3]Dola Ochieng' Henry
[1]Maseno University, School of Computing and Informatics, Department of Information Technology
Private Bag, Maseno, Kenya

Executive Summary: *Cyber Warfare is the current single greatest emerging threat to National Security. Network security has become an essential component of any computer network. As computer networks and systems become ever more fundamental to modern society, concerns about security has become increasingly important. There are a multitude of different applications open source and proprietary available for the protection +-system administrator, to decide on the most suitable format for their purpose requires knowledge of the available safety measures, their features and how they affect the quality of service, as well as the kind of data they will be allowing through un flagged. A majority of methods currently used to ensure the quality of a networks service are signature based. From this information, and details on the specifics of popular applications and their implementation methods, we have carried through the ideas, incorporating our own opinions, to formulate suggestions on how this could be done on a general level. The main objective was to design and develop an Intrusion Detection System. While the minor objectives were to; Design a port scanner to determine potential threats and mitigation techniques to withstand these attacks. Implement the system on a host and Run and test the designed IDS. In this project we set out to develop a Honey Pot IDS System. It would make it easy to listen on a range of ports and emulate a network protocol to track and identify any individuals trying to connect to your system. This IDS will use the following design approaches: Event correlation, Log analysis, Alerting, and policy enforcement. Intrusion Detection Systems (IDSs) attempt to identify unauthorized use, misuse, and abuse of computer systems. In response to the growth in the use and development of IDSs, we have developed a methodology for testing IDSs. The methodology consists of techniques from the field of software testing which we have adapted for the specific purpose of testing IDSs. In this paper, we identify a set of general IDS performance objectives which is the basis for the methodology. We present the details of the methodology, including strategies for test-case selection and specific testing procedures. We include quantitative results from testing experiments on the Network Security Monitor (NSM), an IDS developed at UC Davis. We present an overview of the software platform that we have used to create user-simulation scripts for testing experiments. The platform consists of the UNIX tool expect and enhancements that we have developed, including mechanisms for concurrent scripts and a record-and-replay feature. We also provide background information on intrusions and IDSs to motivate our work.*

Key words: *network intrusion detection, network security monitor, pot scanner.*

I. Introduction

The title of this work is Honey Pot Intrusion Detection System. Intrusion is a major threat to security in computer and network systems. Many software developers keen on inventing applications and mechanisms of combating this dreaded vice in the world of information security have taken this as an area of interest. A network attack is an illegal intentional effort to compromise network security by gaining access to information, manipulating the same thereby rendering a system untrustworthy. (Tech-faq, 2012). A secure network is a key ingredient for any concern to achieve its business objectives. Reliability of a network can be determined by among others, the ability to withstand attacks which may cause partial failure to a distributed system. Even though a hundred percent secure network is yet to be developed, an ideal secure network, should impede intrusion attempts both from within and without to a minimum. It is therefore imperative to detect intrusion and limit its effects on networks, as much as possible. (Scarfone & Mell 2007). The intentions of hackers vary. These may range from an intentional effort to expose confidential material to selfish gain. Irrespective of the cause, attacks pose a threat to a network. These may be in form of injection of malicious code into a computer, unauthorized use of network resources, eavesdropping, DOS attack and installing back door programs into a user's PC in order to enable illegal remote access. (Tech-faq, 2012). It is being realized that network-based security mechanisms such as firewalls are not effective in detecting certain attacks such as insider attacks without generating significant network traffic. Antivirus software, and other defense mechanisms that have hitherto been deployed for network security, are no longer a match for the highly sophisticated attacks. This, arises from the fact that as, experts seek means to tackle intrusion, would be intruders are also working tirelessly hard at devising ways to perpetrate their unlawful activities, necessitating a need for the deployment of IDPS to prevent the intrusion by attackers into what is meant to be a secure system, and the advancement of future safeguards against malicious attacks. (Scarfone & Mell 2007).

Network attacks as mentioned above come in various forms but these can be classified into two major categories i.e. internal and external attacks. Internal attacks are acts perpetrated by authorized users in possession of legitimate rights with ulterior motives, for personal gain. Their administrative rights may allow them to add, delete or modify data. These may be employees within a concern. Often times in a bid to avoid suspicion, they conceal their attacks, making them look as normal processes. (Tech-faq, 2012).

External attacks on the other hand are conducted by third parties outside an organization. It is majorly the work of experienced malicious individuals. Such attacks usually have a predefined procedure and may have monetary value attached to it for the benefit of the individual or may be conducted just for recognition. Software may be employed to identify vulnerable hosts and loop holes within a network before an actual full scale attack is launched. (Tech-faq, 2012). Information security and or networks security has got three pillars all in unison which are the target of network attacks. These are confidentiality, data integrity and lastly availability. In their book Principles of Information Security Whitman and Mattord, define confidentiality as a key aspect of information security. Case in point, it limits information access to authorized users. The network administrators are charged with the responsibility of ensuring that unauthorized users do not gain access to privileged information on a network. Data integrity ensures the consistency of resources on a network. The authenticity of data is brought into question whenever it is altered or modified. Finally the concept of availability on a network ensures information on a network is accessible for consumption by authorized users. The threat is that attackers can render such information unavailable. (Whitman & Mattord 2005).

II. A Review Of Network Intrusion Detection Literature

Information is power; the ability to access it in real time especially over the internet has become important for business with a clientele base widely spread geographically. Presence over the internet has been both a blessing and a curse to many new and growing businesses. Intrusions in computer systems are occurring at an increasingly alarming rate. Some sites report that they are the targets of hundreds of intrusion attempts per month (S. M. Bellovin 2002). Moreover, there are numerous different intrusion techniques used by intruders (P. G. Neumann and D. B. Parker October 1989). The following scenarios are examples of intrusions:

- An employee browses through his/her boss' employee reviews
- A user exploits a flaw in a file server program to gain access to and then corrupt another user's files
- A user exploits a flaw in a system program to obtain super-user status
- An intruder uses a script to “crack" the passwords of other users on a computer
- An intruder installs a “snooping program" on a computer to inspect network traffic, which often contains user passwords and other sensitive data; and
- An intruder modifies router tables in a network to prevent the delivery of messages to a particular computer.

You can easily infer some of the consequences of intrusions from the preceding list. Some additional consequences include loss or alteration of data, loss of money when financial records are altered by intruders, denial of service to legitimate users, loss of trust in the computer / network system, and loss of public confidence in the organization that is the victim of an intrusion (L. D. Gary October 12, 1994).

III. Reasons for Security Detection

One approach to computer security is to attempt to create a completely-secure system. Unfortunately, in many environments, it may not be feasible to render the computer system immune to intrusions, for several reasons. First, system software is becoming more complex. A major challenge programmers face in software design is the difficulty in anticipating all conditions that may occur during program execution and understanding precisely the implications of even small deviations in such conditions. Thus, system software often contains flaws that may create security problems, and software upgrades often introduce new problems. Second, the increasing demand for network connectivity makes it difficult, if not impossible, to isolate and thereby protect a system from external penetration. Finally, a central component of computer systems, the computer network itself, may not be secure. For instance, there are a number of security flaws inherent in the widely-used Transmission Control Protocol/Internet Protocol (TCP/IP) suite, regardless of its particular implementation (S. M. Bellovin April 1989). ISProject proposal 20122013 by Roushdat came in handy for the selection of this project.

In recent news it is coming to light that the number of hackers in the world is not only increasing but also making a shift in global location. *CNN* has recently reported on a mass injection of the hacking community based in and around China, they also speculated and made claims that this was all instigated by the Chinese government to try to begin to gain access to the knowledge and accounts of companies from “The West’’ or the Western world states (Europe & America), and for international commercial and government espionage (Canada Television).
Whether this is true or just speculation it illustrates a point of people becoming more and more aware of the safety of their data, both on the public network (Internet) and on a supposed “Private Computer”. Since these sorts of attacks are becoming prevalent around us, it is imperative that we all have some form of protection to prevent undesired access into our data, from Firewalls on our personal computers to totally isolated systems with little to no

outside access. In addition, the ability of people to be able to identify these attacks would be invaluable. To be able to identify these attacks and manipulations companies that supply the protection equipment are starting to not only turn to the hacking community as the house alarm installers turned to ex-thieves and burglars, but also to the standard user. Each time an attempt is made on a modern machine that runs most windows environments or anti-virus software, a report of this attack is returned to the manufacturer for analysis.

Since these companies are running in such a violent environment, they would also run a lot of what this project is about (IDS systems). The two major approaches that are used by IDSs to detect intrusive behavior are called anomaly detection and misuse detection. The anomaly-detection approach is based on the premise that an attack on a computer system (or network) will be noticeably different from normal system (or network) activity, and an intruder (possibly masquerading as a legitimate user) will exhibit a pattern of behavior different from the normal user (D. E. Denning February 1987). So, the IDS attempts to characterize each user's normal behavior, often by maintaining statistical profiles of each user's activities (T. F. Lunt et al., H. S. Javitz and A. Valdes) Each profile includes information about the user's computing behavior such as normal login time, duration of login session, CPU usage, disk usage, favorite editor, and so forth. The IDS can then use the profiles to monitor current user activity and compare it with past user activity. Whenever the difference between a user's current activity and past activity falls outside some predefined “bounds" (threshold values for each item in the profile), the activity is considered to be anomalous, and hence suspicious.

In the misuse-detection approach, the IDS watches for indications of “specific, precisely represent able techniques of computer system abuse". (S. Kumar and E. H. Spafford, March 17, 1995). The IDS includes a collection of intrusion signatures, which are encapsulations of the identifying characteristics of specific intrusion techniques. The IDS detects intrusions by searching for these “tell-tale" intrusion signatures in the records of user activities.

IV. Network Attacks / Categories of Security Threats and Mitigation Techniques

Today there are numerous attacks both known and unknown which pose a serious threat to corporate networks. In order to protect networks from attack, administrators need to put in place mechanisms to detect the vulnerabilities present on a network and mitigation measures against all forms of inevitable attacks. (Meshram & Nalavade 2011). The reason we use an IDS or Honeypot is to detect any attacks or dangerous activity entering or trying to enter the network behind the IDS. The effectiveness of an IDS can be measured by its ability to detect the usual things as Virus and hacking attacks (Signature based) as well as the less obvious (Anomaly based) .

V. Categories of Security Threats

Security threats can be categorized into four parts, classifications of which threats can be carried out on a network.

Structured threats are conducted by well experienced individuals utilizing highly sophisticated technology to penetrate networks. In isolated cases such attacks are carried out by organized criminal gangs and or industry competitors. Unstructured threats are the kind conducted by inexperienced individuals. Quite often they employ hacking tools such as password crackers and shell scripts. They have the potential to cause grievous harm, thus they should not be underestimated. However a robust security solution has the capacity to thwart such an attack.
The degree of damage posed by internal attack is based on the level of expertise of the perpetrator, who may be a disillusioned employee who has got access to the company’s network.

External threats originate from outside a company’s network and may be the work of either experienced or inexperienced hands, lacking access to the company’s computers or network (Orbit-Computer solutions, 2012).

Physical Layer

This layer could also be referred to as the most changeable and vulnerable layer. It is responsible for transferring data over network communication media. Trivial incidents like abruptly unplugging the computer power cord or the network cable could damage the computer and cause a great untraceable havoc on a network. (Reed, 2003)

The physical layer faces a host of vulnerabilities which are potential causes of network insecurity without proper stop gap measures. These vulnerabilities include but are not limited to damage of hardware and data including physical theft, power loss and loss of environmental control, input logging keystrokes and undetectable interception of data. Mitigation for the above varies. Data storage cryptography, PIN and password secured locks, electromagnetic shielding and biometric authentication systems, video and audio surveillance plus perimeter and enclosure lock are among the measures that can be used to secure a network from potential and active threats to the physical layer.

Application Layer

This is the closest a user can get to interact with the application and networks. An application that is not robust or otherwise unauthenticated could be the weakest link over the network and thus could potentially be a prime target i.e. if a username or password is not required, an intruder would have no challenge in guessing file names in TFTP protocol.

Standard security control is bypassed through the backdoor and application design. In the event that security controls force approach is not adequate, the results can either be insufficient access or excessive access. Whenever application security is too complex, users often have a challenge in understanding it and logic often times could cause programs to crash or behave undesirably. According to (Reed, 2003) using baseline in measuring application implementation, such as application codes review and standard testing using host-based firewall system to regulate traffic, application activities and inquiries monitored by the use of IDS systems, are all means of controlling vulnerabilities of application layers.

Mitigation against Application Layer Attacks

Risks associated with application layer attacks can be brought under control by implementing the following measures; a)subscribing to mailing lists that frequently broadcast network vulnerabilities b)deploying IDPS on the network c) reading Operating System and network log files and d)Updating Operating System with patches from reliable vendors. (Knap/SecTools 2010.)

Buffer Overflow

This is a common threat on networks that occurs when a program or application saves more data in a buffer memory than its intended capacity. (Fu-Hau & Tri-cker 2008,4)

According to Fu-Hau, et al (2008,6) buffer overflow attacks often occur as a consequence of bugs and proper use of programming languages that are not memory safe such as C and C++ . Attackers can inject code into an unsuspecting victim's network system and contaminate services of the host thereby be able to manipulate services running in a network at will, due to the presence of bugs.

Reconnaissance Attack

Often overlooked by administrators because of the form it takes to penetrate the network. Hackers use reconnaissance attacks to gather information about a particular network, that would be useful in accessing the network and or carry out a DOS attack (Cisco, 2005).

Packet Sniffers

Sniffing is a process of eavesdropping packets and analyzing traffic in a network.

This is a tool used by network administrators to capture packets travelling across a network of TCP/IP layer and for detecting any kind of fault on the network. Attackers on the other hand use it for eavesdropping and capturing packets sent across networks (Cisco 2007).

Mitigation against packet Sniffer Attacks

Mitigation against packet sniffing attacks can be achieved by the use of several techniques including: Authentication, Anti-sniffer tools and Cryptography (Cisco 2007).

Another alternative would be to use anti-sniffer tools, solely to detect sniffers on a network but not to completely prevent threats. They are ideal for detecting changes in response time of packets sent or received from a host (Colasoft, 2012).

Secure Remote Administration Using SSH

SSH has replaced telnet as the best application for providing remote router administration with connections that support session integrity and privacy. It uses port 22 and offers similar functionality to an outbound telnet connection, except that the connection is encrypted. This allows for secure communication over an insecure connection (Lawrence 2000, 47).

Port Scans and Ping Sweeps

These applications run a battery of tests against hosts and network devices to identify vulnerable services that need to be hardened.

Affiliated attacks can attempt to; identify all services on the network, identify the operating system on the network, Identify vulnerabilities on the network and Identify all hosts and devices on the network (Cisco 2007).

Mitigation against Port Scans and Ping Sweeps

It would not be practical to prevent attackers from carrying out port scans and ping sweeps on a network. Deploying an IDPS in a network structure can help control attacks. An IDPS would notify the network administrator whenever such an attack is in progress. The network administrator would then be better prepared for a large scale impending attack (Cisco 2007).

Internet Information Query

"WHOIS" is the attackers' weapon of choice used to view addresses by DNS queries, so that they can present a targeted network's live hosts. Such queries reveal the range of IP addresses and the domain associated with the addresses, valuable information that could be utilized to launch an attack (De Capite 2006).

Access Attack

This can be launched both from within and without a network with different reasons for each attack. The intruders would gain entrance into a network in an unauthorized manner to steal vital information and engage in the destruction of resources that could potentially lead to their identification (Cisco, 2007).

Access attacks include but are not limited to;

Password Attacks

Passwords are secret words or strings of characters that are used for authentication and gaining access to a

computer system or network (Whitmann & Mattord 2005). Network intruders endeavor to gain unauthorized access to a computer or network system by several methods or guessing user ID's and or administrator password (Pfleeger, 2006).

Brute force attacks is an effort involved in guessing all possible dictionary words until the right password or authorized user or administrator is found. Presently, intruders use brute-force, a more sophisticated method in carrying out attacks. The tool searches for detailed information using combinations of character sets to work out every possible password made up of the victims information.

A dictionary attack is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password.

Network and security administrators can counter password attacks using the following techniques:

a) Guiding users on how to formulate un-guessable strong passwords. A combination of lower and upper case letters, special characters and numbers would be difficult to guess. b) Limiting the number of unsuccessful login attempts. For example after three unsuccessful login attempts or if the correct login details is incorrectly applied an account is disabled. c) Authorized users should be forbidden from sharing passwords. d) End user passwords should be regularly changed. Example, systems could be programmed so as to prompt users to change their passwords every so often. e) Passwords should be encrypted over a network (Whitman & Mattord, 2005).

Trust Exploitation

Hackers leverage on the existing trusting relationships within a network to launch an attack. For instance an attack can be witnessed in a perimeter network connected to a corporate network. Some of the trust models that exist include; Windows, NIS+, NIS, Active directory, Linux and Unix domains.

An effective means for mitigation against trust exploitation attack is enforcing strict protocols on trusted hosts within a network (Cathayschool 2010).

Port Redirection

This is a kind of exploitation attack which uses a fragile host in passing traffic that would otherwise be dropped via a firewall. A host on the outside can contact the host on the public services segment, DMZ (Host1), but not the host on the inside (Host 2). The host on the public services segment can be reached by host on both the inside and outside. In the event that hackers successfully compromise the public services segment host, they would be able to install software to channel traffic from the outside host directly to the inside host, with neither communication failing to agree with the rules implemented by the firewall.

The outside host has through this achieved a good network connection to the inside host simply through the port redirection process on the public services host. Netcat is a good example of an application that can render this service (Stuart, 2011).

Mitigation against port re-direction attack can be done by double checking appropriate utilization of trust models. Better still, deployment of host-based IDPS can detect an attack and prevent installation of malicious software on a host (Orbit-Computer-Solutions, 2011).

Man in the Middle Attack

MItM attacks have got many faces including hijacking of on-going sessions in a bid to access internal network resources, traffic analysis so as to derive information from the network and its users, denial of service, theft of information, corruption of transmitted data and the introduction of new information into network sessions. It is a situation where an attacker intercepts communication between two legitimate hosts. Employees of ISP's have the capacity to access all network packets and carry out all of the above operations.

In WAN mitigation against MItM attack would be achieved by implementing VPN tunnels in a network. VPN tunnels only allow attackers to see encrypted unreadable packets. In LAN, configuring port security on LAN switches would be of help against MItM attacks (Microsoft TechNet 2012).

Denial of Service Attacks

DOS attacks are very common on web pages, computer and network systems. Here, computers or network resources are consumed by attackers' tools thereby preventing legitimate users from accessing information, rendering services unavailable.

In certain cases attackers target an entire network, blocking outgoing and incoming traffic. Some of the techniques used to implement DOS are; Flooding, Ping of Death or SYN. (IBM, 2004)

DOS attacks may consist of the following;

IP Spoofing

This is a technique used to acquire unauthorized access to computers. Hackers first use a variety of techniques to look for an IP address of a trusted host including sending illegitimate messages to a computer with an IP address showing that the message is coming from a reliable and trusted host, they then modify their packets headers to appear as if they are originating from that trusted host.

Other unsuspecting hosts could also be dragged into the net in order to generate traffic and create an impression like the origin is trusted, only to cause more harm by flooding the network.

Mitigation against Distributed Denial of Service Attacks

Mitigation against DOS attack can be achieved by implementing anti-DOS software applications on a

network. Organizations can also instruct ISP's to implement traffic rate restrictive software, which controls the quantity of traffic transmitted across a network (Orbit-Computer Solutions, 2011).

Worms Viruses and Trojan horse Attacks

Using antivirus software, some threats categorized as minor vulnerabilities can be solved, thereby reverting the affected machine to its default factory settings.

A virus is a malicious software or program attached to a file spreading from one computer to another causing undesirable function on a user workstation. Workstations or network resources can be infected if end users intentionally run infected programs or unknowingly download software. A human aspect is required, i.e. introduction of an infected file either through an email attachment or through a CD. (Whitman & Mattord 2005).

A worm is a subclass of a virus which can affect computer systems. Worms however are distinct in the manner in which they spread compared to viruses. Worms are self replicating malware which execute arbitrary code and also installs copies of themselves on the affected PC's memory, which in turn spreads to other hosts on the network. (De Capite, 2006)

The only difference between Viruses and Worms is that while the former requires human interaction for propagation, the latter greatly benefit from automatic file transmissions to propagate itself.

Trojan horses are hacking programs that are non-self replicating which gain privileged access to the operating system while appearing to perform a desirable function only to drop a malicious payload, often including a backdoor allowing unauthorized access to the target's computer.

Prompt action is required in order to stop the spread of malicious code in a network. Worms, Viruses and Trojan horses can be controlled through;

a) Ensuring that the network Operating System is up to date.
b) Installing reliable antivirus software and regularly updating the signatures.
c) Scanning infected computers and disconnecting them from the network if need be.
d) Implementing host-based IDPS, to detect and prevent malicious code attacks (Orbit-Computer-Solutions.Com 2011).

Intrusion Detection and Prevention System

The fusion of intrusion detection and intrusion prevention has brought about intrusion detection and prevention system widely used today.

Intrusion detection on a network is basically monitoring all activities searching for traces of violations of security policies, peculiar to an organization.

Such malicious activity can originate from within the organization, initiated by authorized users who may be misusing their privileges or trying to gain access to vital resources in domains beyond their jurisdictions. Alternatively, they may originate from external users trying to gain illicit access through extranet or internet.

According to Scarfone & Mell in "Guide to Intrusion and Prevention Systems", recent research has shown that the greatest degree of malicious activity on any given work is often perpetrated by insiders.

Intrusion prevention on the other hand is a preemptive approach to network security used to identify potential threats and respond to them swiftly.

The primary functions of an IDPS are;

- Identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.
- Identifying problems with security policies
- Documenting existing threats
- Deterring individuals from violating security policies.

IDPS Detection Methodologies

There are three methodologies i.e. stateful protocol, signature-based detection and anomaly based detection. (Wikipedia)

Stateful Protocol

Stateful protocol analysis provides important capabilities for understanding and responding to attacks. It is designed to rely on software developer's general profiles that spell out how "particular protocols should either be used or not used"

This protocol can spell out unpredictable sequences of commands such as issuing the same command repeatedly alongside performing authentication and keeping records of each activity by the authenticator and recording any suspicious activity. (Scarfone & Mell, 2007, 2-6)

In addition, it can detect variations in command lengths, minimum and maximum values for attributes, and other potential anomalies that might not be detected by signature-and anomaly-based systems.

In spite of all these benefits, there are some short comings. The greatest of which are resource requirements. Tracking and analyzing information for systems requires meaningful resources. As performance capacity of processors and networks increase, the challenges associated with resource usage intensify. Another challenge in implementing stateful protocol analysis with IDPS is that malicious traffic may correctly make use of system protocols and therefore successfully penetrate without being detected. (Scarfone & Mell 2007, 8-10)

Signature Based Detection

Signature based protection is a simple detection method designed to react to known threats but unreliable at detecting unknown threats. Very often attackers conceal their activities using avoidance skills with the intention of deceiving security protocols. A normal signature may be an email titled "Free pictures" or "Freepics.exe" both typical features of malicious code. The same signature slightly modified to read "Freepics2.exe", would not be a match to any known threat. Thus, it would penetrate without detection. (Scarfone & Mell 2007, 17)

Anomaly Based Detection

According to Stuart, (Stuart 2011) anomaly based detection is a means of monitoring network or system activity and classifying these as either normal or anomalous based on the profiles created for each user group and mechanism on the system. An alarm is triggered off in the event that significant deviations from normal pre-generated "profiles" are observed. (Stuart 2011) This is because anomaly based IDPS have profiles signifying normal behavior of end users, service hosts or applications. (Grand 2012).This technique is deemed efficient since it is not centered on customized profiles. It has the capacity to potentially detect attacks the first time it is perpetrated and would initiate logs to system administrator whenever a new type malicious code infects the system. Similarly if an authorized user initiates activities beyond his/her jurisdiction an alarm would be triggered making it easy to identify internally initiated attacks (Carter 2002).

However its major limitation is its complexity and perhaps the difficulty of associating a specific event with an alarm, unless an actual test is conducted. Case in point, malicious attacks that are too close to normal user activities might go undetected.

Functions of IDPS

Today most organizations typically have firewalls on their networks which filter packets and checkmate traffic but most still suffer intrusions on their network. IT professionals painfully aware of the need for additional protective technologies on a network have come up with IDPS.

Heralded as a cost effective way to block malicious traffic, detect malicious code, serve as a network monitoring device, act as a network sanitizing device and assist in policy compliance requirements. IDPS can be designed to detect violations of organizational security and acceptable user policy like restriction on transfer of inappropriate material over a network or downloads of software onto company desktop or user laptop (Grand 2008).

Furthermore IDPS can also recognize reconnaissance activities intent on identifying vulnerable hosts, which may signify that an attack is looming. For example it might be able to detect and block such attempts and notify security administrators who may then enable other security controls to counter the attack over and above producing logs of network activity (Kizza 2005).

Table 1. Provides a comparison of the IDPS technologies, with particular reference to their strengths.

Table 1. Comparison of IDPS technologies (Scarfone & Mell 2007)

Type of IDPS Technology	Type of malicious activity detected	Scope per sensor or agent	Strength of IDPS
Network Based	Network, transport and application TCP/IP layer activity	Multiple network subnets and groups of hosts	Able to analyze the widest range of application protocols: only IDPS that can thoroughly analyze many of them
Host Based	Host application and OS activity, network, transport, and application TCP/IP layer activity	Individual hosts	Only IDPS that can analyze activity that was transferred in peer encrypted communications
Wireless	Wireless protocol activity : unauthorized WLAN in use	Multiple WLANs and groups of wireless clients.	Only IDPS that can monitor wireless protocol activity
NBA	Network, transport and TCP/IP layer activity that causes anomalous network flow.	Multiple network subnets and groups of hosts	Typically more effective than the others at identifying reconnaissance scanning and DOS attacks and at reconstructing their malware infections

VI. IDPS Add-Ons

Honeypot

In essence, a Honeypot is a resource which is intended to be attacked and compromised to gain more information about the attacker and his attack techniques. It can also be used to attract and divert an attacker from the real targets. It will sit idle listening and waiting for something of interest to trigger its sensors and cause a reaction that will produce some information or physical grabbing of its target. But in order to do so, the administrator must properly build the Honeypot machine is such a way that the machine fools the attacker into believing that it's the real system so that he/she can effectively log information about the attackers' behavior. The administrator can then learn about the vulnerabilities of the current system and redesign it to be more secure. The

idea of the Honeypot is all around us, in the natural and un-natural world, even though we may not see them at first glance. Honeypot's are not a new thing; we can take natural examples and adapt them to work for the un-natural application.

In the natural world, there is one example above all others that people will see but not realize that it can relate to a Honeypot. This example is the *Venus Fly Trap.* The Venus is one of the very, very, very rare examples of a *carnivorous* plant (i.e. it eats meat), what it does is it will sit idle blowing in the wind, but it attracts flies and other small insects to it by secreting a sweet scented and tasty liquid from its opening.

The leaves of Venus' Flytrap open wide and on them are short, stiff hairs called trigger or sensitive hairs. When anything touches these hairs enough to bend them, the two lobes of the leaves snap shut trapping whatever is inside in less than a second. (botany.org)

Once something enters the mouth it will crawl to the bottom and along the way will brush against hairs triggering the trap and closing the mouth. Its prey is then consumed and digested for the plant to survive.
This is not quite the same as the Honeypot in IT, but the concept is very similar, and can almost simulate identical action depending on the system that is implemented (Wikipedia).

System Integrity Verifier

System Integrity Verifier is software that monitors critical files in a network to establish whether they have been accessed or altered plus a host of other sensitive system components or activities e.g. it would be able to tell when an authorized user acquires administrator rights enabling him/her access critical files in a network. Plus, it monitors system registries to find known signatures. An example of SIV is Tripwire, which monitors system files to detect Trojan versions of system binaries (Kizza, 2005).

Log File Monitor

Log file monitor software operates first by creating a record of log files generated by network services. Thereafter, it monitors records looking for system developments in the log files that would suggest that an intrusion is in progress (Kizza, 2005).

Network Forensic Analysis Tool

This is a software application that captures network packets and analyzes them according to authorized users' needs. Similar to honey pots, it is used to learn about attackers' modes and methods of network attack (Kizza, 2005).

Challenges and Limitations of IDPS

Although these technologies are gradually gaining recognition and acceptance among system administrators as defensive and preventive mechanisms for corporate networks, they are faced by a few challenges. IDPS sensors should be placed in network sections where they can sense and monitor traffic. However, the reverse is witnessed in switched networks where sensors are protected from network traffic. This limits their functionality. Hence, they cannot therefore assure complete accuracy in the detection and prevention of attacks (Kizza, 2005).
Secondly, IDPS technologies are yet to gunner the capacity to counter large scale attacks. Given that IDPS scans every packet, contact point, host and traffic trends in a network, the demand on a large network would be phenomenal. The net effect would be failure to provide real time detection and prevention (Scarfone & Mell, 2007).

Third, IDPS are still reactive rather than proactive i.e. they are signature based. The signature database needs to be updated whenever a different kind of attack is detected. The literal meaning of this is that even with IDPS installed, intrusions might still be witnessed in a network, since the frequency of signature updates vary from vendor to vendor, thereby limiting effectiveness (Scarfone & Mell, 2007).

Fourth, some element of human intervention is required for success with IDPS technologies. Optimum security may in addition require the attachment of add-on applications (Grand 2012).

Fifth, IDPS technologies are susceptible to various forms of attacks. Attackers can render a sensor blind to malicious activity by generating abnormally large volumes of traffic through a DOS attack in a bid to wear out an IDPS sensor resource (Kizza, 2005).

Finally, false alarms by an IDPS sensors or agents are inevitable. These are categorized into two i.e. false positives and false negatives. False positives occur when authorized users' activities falsely activate an alarm. On the other hand, a false negative occurs when an IDPS fails to activate an alarm or detect malicious activity on a network. False alarms are a major limitation of this technology, often confusing administrators, on when to act appropriately (Bejtlich, 2012).

IDPS Components

All the types of IDPS technologies share the same basic components i.e. sensors or agents, management servers, multiple consoles and database servers (Zaugg, 2010).

Sensors and agents play the role of detecting malicious activity on a network. The only difference is that Host-based IDPS use agents whereas network-based, wireless and NBA use sensors. IDPS technologies can be deployed in two modes: inline and passive. In the inline mode, network traffic passes through a sensor where it is analyzed for any malicious activity. Reason being, to stop attacks and control access to the network by blocking traffic. While in the passive mode, sensors are deployed at key locations on a network. Traffic do not pass through

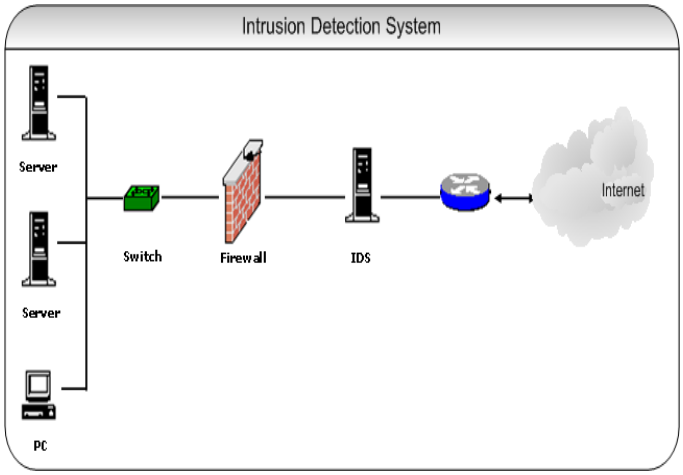
the sensors, rather they analyze a copy of network traffic for malicious activity (Bejtlich, 2012).

Management servers are centralized devices tasked with receiving information from sensors or agents, process, analyze, correlate and manage this information. In larger network environments, there are several management servers that match information received from multiple sensors or agents compared to small networks (Cisco, 2007).

A database server is used as a storage area for information received and recorded by sensors/agents or processed by management servers (Bejtlich, 2012).

Console is an application that provides an interface for the administration of IDPS such as configuring sensors or agents, while others are used for monitoring and analyzing packets in a network. These consoles can either be combined or used individually. (Endorf & Eugene & Mellander, 2003)

Conceptual Framework



Source: Managing and Troubleshooting Networks Myers, M (2009)

IDS is the front raw warier in the fight against security threats. This front raw warier needs to overcome a few challenges in order to carry out its responsibilities successfully. Like the old story if an IDS shouts "wolf wolf" frequently and incorrectly no one is going to believe it. Security staff needs to analyze alerts generated by IDS. Each alert demands resources like time and effort. A large number of false positives make the life's of staff horrifying, since they are benign but have been identified as attacks. To overcome the false positive problem, we need to understand its causes. An IDS identifies attacks by differentiating them from benign traffic. The only problem with the signature based approach is creation of precise signature. If a signature is too specific, it cannot identify a slightly modified attack. The attacker would perform slight changes in the attack pattern and the attack would go through unnoticed On the other hand, if we design too generic a signature, it will detect attack variations but increases the possibility of false positives. Such a generic signature identifies benign traffic as attacks because of a similar pattern. Context sensitivity is also another reason for generating false positives. Windows can use NetBIOS in LAN environment but such traffic cannot present on internet. Hence depending on the context, same network traffic can either be normal or an attack. Intrusion detection systems come with their default configuration. In many cases, these default configurations result in a number of false positive alerts. For the efficient configuration of an IDS, it is essential to understand the network topology and host vulnerabilities.

In related work, Sandhya (Sandhya, 2007) have proposed ensemble architecture for IDS. They have suggested a hybrid system based on Support Vector Machine and Decision tree. Using the hybrid approach they have tried to maximize detection accuracy and minimize computation complexity. Witcha, (Witcha) have proposed Rough-Fuzzy hybrid algorithm for computer intrusion detection. They have applied rough set based methods to identify subset of features and fuzzy c-means for intrusion detection.

Huy Anh (Huy Ahn, 2008) have suggested classifier detection model which uses data mining techniques. They have evaluated performance of comprehensive set of classifier algorithms using KDD99 dataset. From the evaluation results they have proposed two classifier algorithm selection models. Prasad (Prasad, 2008) have proposed intrusion detection using Data Mining and Genetic Algorithm based on Fuzzy Logic. Their model uses anomaly detection based on fuzzy association rules which use genetic programming. Jing Hiao-Pei (Jing Hiao-Pei, 2010) have proposed Immunity Intrusion Detection Model based on Genetic Algorithm and Vaccine Mechanism. Other researchers have also used Genetic Algorithm for Intrusion Detection. In our proposed model, we are suggesting Genetic Algorithm and Neural Network based solution for reducing false positive rate. The basic idea is to get the benefit of these two prominent soft computing techniques. The major components in our solution are;
Network traffic is handled by preprocessing component. This module is responsible for clean input data as well as

handles missing and incomplete data. It collects network packet and generates records required for further processing. Initially one can start with default configuration but it is highly recommended to modify configuration according to network topology, hosts existing, services running and other parameters. Vulnerability scanner tool recommended to collect such data and configuration should be modified by Intrusion Detection Analyst or Security Staff. A properly configured preprocessing unit will help in reducing false positive rate generated due to network topology and context sensitivity. Detection engine collects records from preprocessing unit. This part is heart of the solution. We can divide attacks in four major classes: DOS, remote to local, user to root and probe. Genetic Algorithm and Neural Network both generate minimum false positive for certain attack classes while generates significant false positive for other classes. So we have assigned weight for each attack class to both classifiers. Analysis engine pass on the records to Genetic Algorithm for Intrusion Detection. Optimized Genetic Algorithm classifies records in various classes like normal Record, suspicious record and possible attack record for each attack class. Based on record type and attack type, weight is calculated for suspicious records and possible attack records.

Normal record identified by Genetic Algorithm is excluded from further processing. Suspicious record and possible attack record pass on to Neural Network for further processing. Neural Network also classifies record in to normal record, suspicious and possible attack record for each attack class. Combiner component is responsible for combining results produced by Genetic Algorithm and Neural Network. It passes on these processed results to response unit. Response unit pass on results to Alert Monitoring System. It also transfers conflicting results Intrusion Detection Analyst for verification. Intrusion detection analyst may send manual response to Alert Monitoring System. If required Intrusion Detection Analyst can adjust configuration file and or database.

In our proposed model we have tried to reduce false positive rate in three different stages. In the first stage preprocessing mechanism reduces false positive. In the second stage Genetic Algorithm and Neural Network identifies attacks and reduce false positive by further processing. In the third stage, Intrusion Detection Analyst identifies false positive and adjust system accordingly. IDS is one of the critical components in computer network security. It however requires to address challenges like false positive to achieve the desired goal. Here, we have proposed a three stage solution for reduction of false positive rate. Preprocessing stage reduces topological and context sensitive false positive. We suggest Genetic Algorithm and Neural Network for Intrusion Detection. Collectively these two techniques significantly reduces false positive rate. Finally, Intrusion Detection Analyst helps reduce false positive rate significantly.

VII. The Results

Presentation of Results

The presentation of results by Honeypot IDS is analyzed in terms of the interface of the system and output. This includes user activities. The following are the results after the implementation of Honeypot IDS.

System Interface

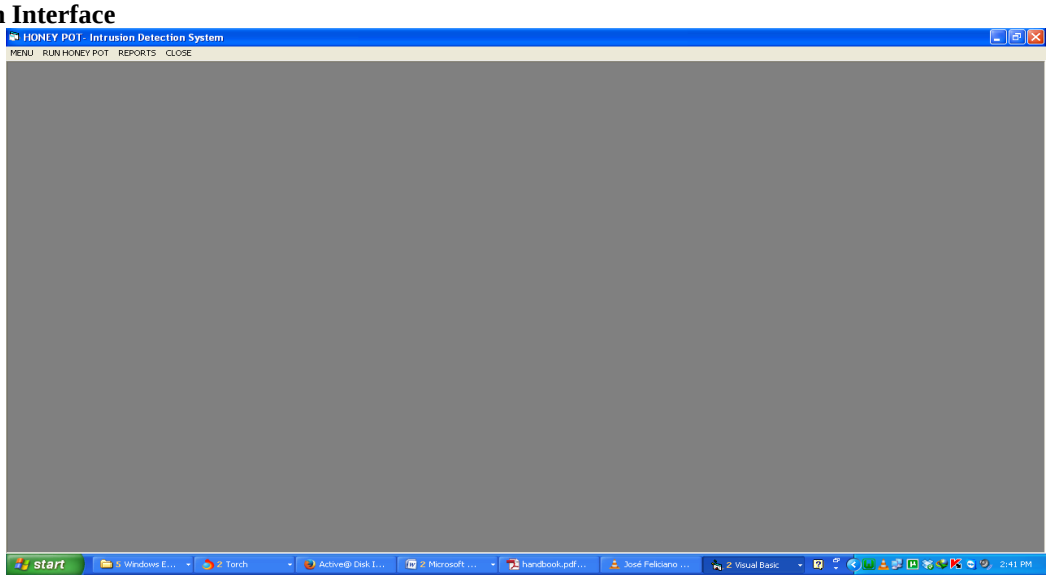
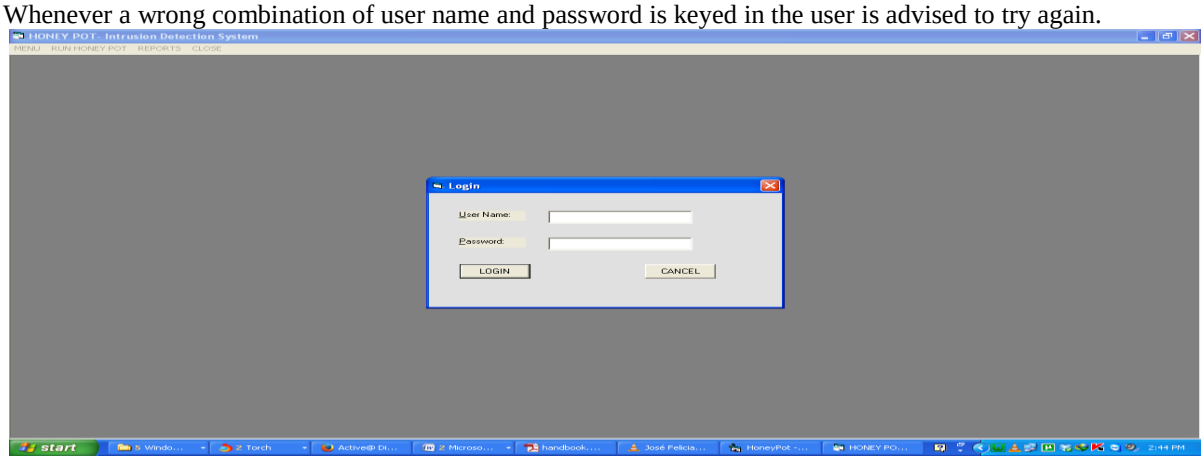


Figure 4. System interface

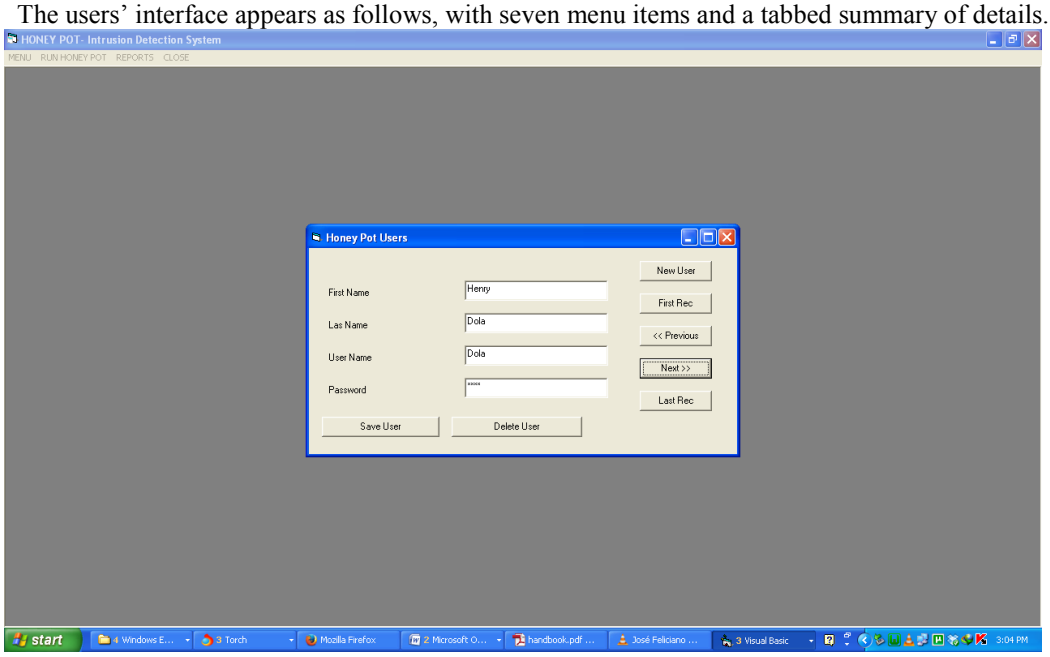
Login Form

Only authorized users with the correct user name and password have rights to access the system. Whenever a wrong combination of user name and password is keyed in the user is advised to try again.



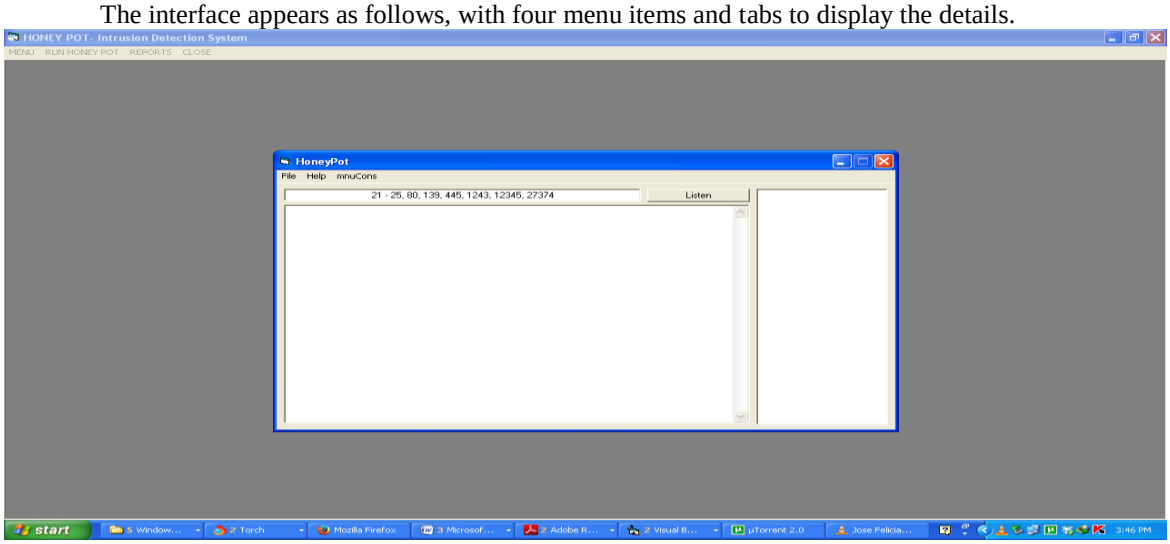
Honey Pot Users

The users' interface appears as follows, with seven menu items and a tabbed summary of details.



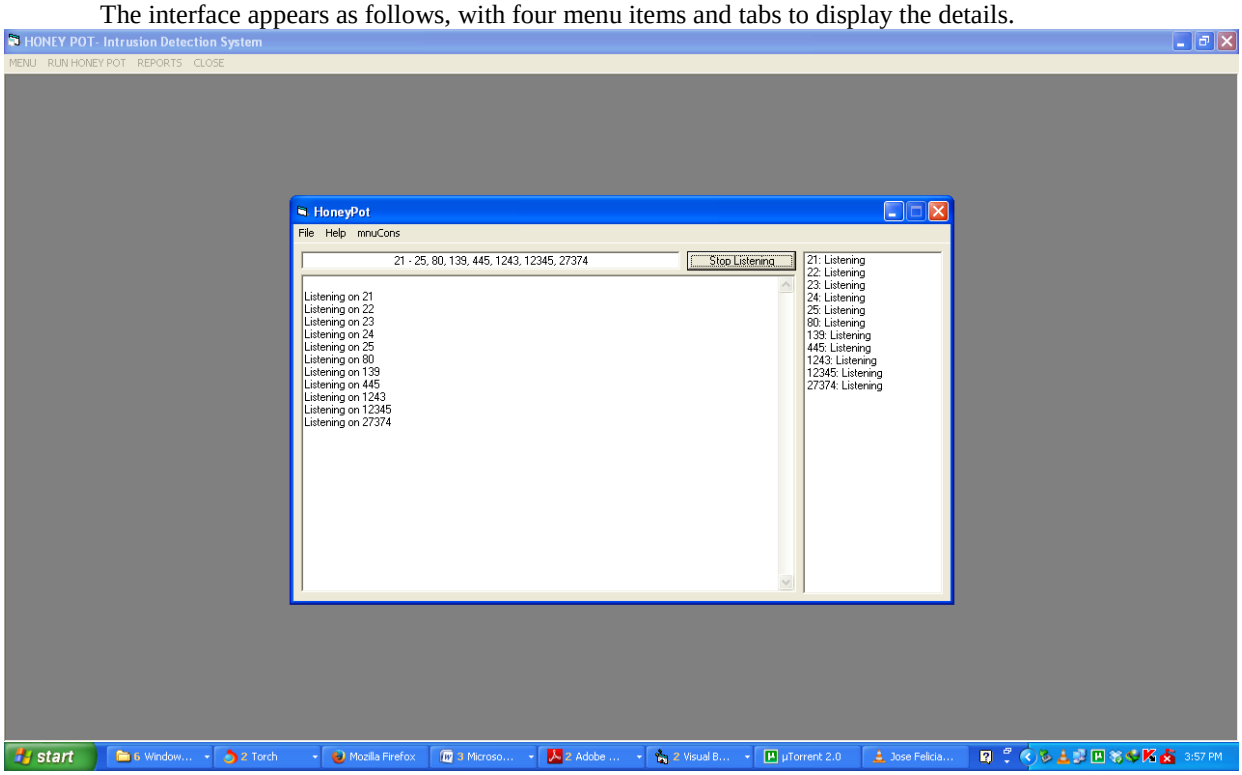
Run Honey Pot

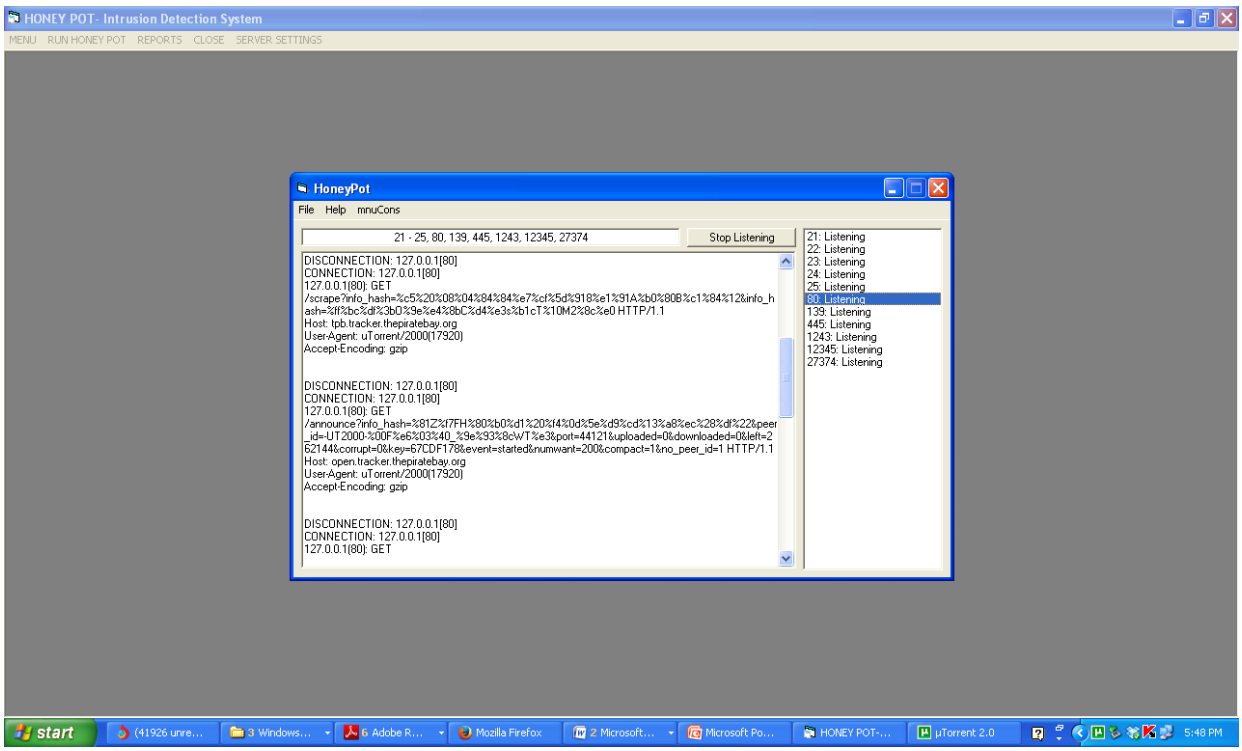
The interface appears as follows, with four menu items and tabs to display the details.



Listen to Ports

The interface appears as follows, with four menu items and tabs to display the details.





VIII. Conclusion

The main motivating factor towards developments of the HIDS is to enable users have the confidence and or assurance of safety while online. A lot still needs to be done in this field in order to make available technology effective, starting with user sensitization. The researcher acknowledges the fact this system cannot presently contact (raise an alarm) an individual away from his/her PC . The researcher therefore suggests that for further research, be conducted on this area.

IX. Recommendations

Cyber security training to all online users is advised

References

Printed

[1] Serianu (2012) Kenya Cyber Security Report: Getting Back to the Basics Retrieved from: Kenya Cyber Security Report (1st ed.)
[2] L. D. Gary (October 12, 1994), talk presented in "Crime on the Internet" session, 17th National Computer Security Conference, Baltimore, MD.
[3] H. S. Javitz and A. Valdes, (May 1991) "The SRI IDES Statistical Anomaly Detector," Proc.,
[4] IEEE Symposium on Research in Security and Privacy, Oakland, CA, pp. 316-376.
[5] P. G. Neumann and D. B. Parker , October 1989., "A Summary of Computer Misuse Techniques," Proc., 12th National Computer Security Conference, Baltimore, MD, pp. 396-407
[6] S. M. Bellovin (September 1992), There Be Dragons," Proc., Third USENIX UNIX Security Symposium, Baltimore, MD, pp. 1-16,
[7] S. M. Bellovin (April 1989), "Security Problems in the TCP/IP Protocol Suite," ACM Computer Communication Review, vol. 19, no. 2, pp. 32-48.
[8] D. E. Denning February 1987, "An Intrusion-Detection Model," IEEE Transactions on Software Engineering, vol. SE-13, no. 2, pp. 222-232.
[9] Bejtlich Richard (2012) The Practice of Network Security Monitoring : Understanding Incident Detection and Response No Starch Press , USA.
[10] Whitman, Michael E. & Mattord, Herbert J. (2012) Management of Information Security. (3rd ed.) Thomson Learning Inc., Massachusetts, USA.
[11] Bhatti D., Virparia P. & Patel B. (2012) Conceptual Framework for Soft Computing based Intrusion Detection to Reduce False Positive Rate Retrieved from: International Journal of Computer Applications (0975-8887) Volume 44-No 13, April 2012
[12] Meshram, B.B. & Nalavade, Kanini (2011) Layered Security Framework for Intrusion Prevention Retrieved from IJCSNS International Journal of Computer Science and Network Security, Vol.11 No6, June 2011.
[13] S. Kumar and E. H. Spa_ord, (March 17, 1995) "A Software Architecture to Support Misuse Intrusion Detection," Technical Report CSD-TR-95-009, Purdue University.
[14] Stuart, Jacobs (2011) Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance. John Wiley & Sons, Inc. New Jersey, USA.
[15] Xiao-Pei J. & Hou-Xiang W. (2010) A New Immunity Intrusion Detection Model Based on Genetic Algorithm and Vaccine Mechanism, Retrieved from: IJ. Computer Network and Information Security, 2010,2, 33-39
[16] Nguyen H. & Choi D.(2008) Application Of data Mining to Network Intrusion Detection : Classifier Selection Model, APNOMS '08 Proccedings of the 11th Asia Pacific Symposium on Network Operations Management: Challenges for Next Generation Network Operations and Service Management, ISBN 978-3-540-88622-8,2008
[17] Fu-Hau Hsu, Fanglu & Tzi-Chiueh (2008), Scalable Network-based Buffer Overflow Attack Detection. IEEE Xplore, New York, USA
[18] Serena (2007) An Introduction To Agile Software Development : Retrieved from Serena.com. Serena software, Inc.
[19] T. F. Lunt et al.,(May 1990) "A Real-Time Intrusion Detection Expert System(IDES)," Interim Progress Report, Project 6784, SRI International.
[20] Scarfone, K & Mell, P (2007) Guide to Intrusion and Detection Systems: Recommendations of the National Institute of Standards and Technology. Gaithersburg, USA.
[21] Sandhya P, Abrahamb A., Grosanc C. & Thomasa J. (2007) Modeling Intrusion Detection System Using Hybrid Intelligent Systems Retrieved from : Journal of Network and Computer Applications 30 (2007) 114-132,2007
[22] Witcha C., Abdullah A., Noor M., Chimphlee S. & Srinoy S. (2007) A Rough-Fuzzy Hybrid Algorithm for Computer Intrusion Detection Retrieved from: The International Arab Journal of Information Technology, Vol 4, No. 3, July 2007.
[23] Pfleeger, C.P. & Pfleeger, S.L (2006) Security in Computing (4th ed.) Syngress Publishing, Inc. Newyork, USA.
[24] Duane De Capite (2006) Self-Defending Networks: The Next Generation of Network Security Cisco Systems Inc., 170 West Tasman Dr. San Jose, USA.
[25] Kizza, Joseph Migga (2005) Computer Network Security. University of Tennessee Chattanooga, Chattanooga, TN, USA
[26] Whitman, Michael E. & Mattord, Herbert J. (2005) Principles of Information Security. (2nd ed.) Thomson Learning Inc., Massachusetts.
[27] Endorf, carl & Eugene Schultz & Jim Mellander (2003) Intrusion Detection and Prevention McGraw-Hill Osborne Media, New York, USA.

Not Printed

[28] Colasoft (2012) Network Sniffer Introduction. Retrieved from: http//www.colasoft.com/resources
[29] UKDiissertations (n.d.). Intrusion Prevention Security Information Systems Dissertations: Retrieved from http://www.ukdissertations.com/dissertations/information-systems/intrusion-prevention-security.php
[30] Knap/SecTools (2010) Top Web Vulrenabilities. Retrieved from http://sectools.org/web-scanners.html
[31] Cisco Security (2007) Cisco Networking Academy Program Retrieved from: http://cs.mty.itesm.mx/cursos/ccnp/en_CCNP_ISCW_v5030/ch1/main.html
[32] IBM.COM(2004) Lessons in Secure Messaging Using Domino 6 Retrieved from: http://www.ibm.com/developerworks/lotus/library/securemessaging/
[33] Reed Damon (2003) Applying the OSI Seven Layer Network Model to Information Security Retrieved from http://www.sans.org/reading_room/whitepapers/protocols/applying-osi- layer-network-model-information-security_1309
[34] Cisco Security (2003) Securing Cisco Network Devices. (v 1.0 ed) Retrieved from: http://www.scribd.com/doc/985242/securing-Cisco-Network-Devices-SNDv1-0
[35] Carter, Earl (2002) Intrusion Detection Systems: Retrieved from Ciscopress.com: http://www.ciscopress.com/articles/article.asp?p=25334
[36] Lawrence , Teo (2000). Network Probes Explained: Understanding Port Scans and Ping Sweeps Retrieved from : http://www.linuxjournal.com/article/4234
[37] Rehman, R.U. Intrusion Detection Systems with Snort Prentice Hall PTR Upper Saddle River, New Jersey 07458 www.phtr.com
[38] Brandel, Mary (n.d). How to Compare and Use Wireless Intrusion Detection and Prevention Systems Retrieved from CSO Online: http://www.csoonline.com/article/502268/how-to-compare-and-use-wireless-intrusiondetection-and-prevention-systems

[39] Grand, Alberto (n.d.). Intrusion Detection and Prevention Systems Retrieved from: http://www.scribd.com/doc/2096981/Intrusion-Detection-and-Prevention-Systems.
[40] Canada Television. (n.d.). Chinese hackers try to access Canadian gov't data. Retrieved from CTV News: http://www.ctv.ca/CTVNews/TopStories/20110216/china-hackers-canada-finance-department-110216
[41] Orbit-Computer Solutions. (n.d.). Threats to Physical and Network Infrastructure Retrieved from: http://www.orbit-computer-solutions.com/Threats-to-Physical-and-Network-Infrastructure.php
[42] Violino (n.d.). How to Use Network Behaviour Analysis Tools Retrieved from Network world: http://www.networkworld.com/news/2008/111008-how-to-use-network-behavior.html
[43] Brecht, Daniel (n.d.). Network Intrusion Detection Prevention Retrieved from ehow: http//www.ehow.com/about_6661697_network-intrusion-detection-prevention.html
[44] Microsoft Technet (n.d.) Common Types of Network Attacks: Retrieved from: http://technet.microsoft.com/en-us/library/cc959354.aspx
[45] Snort team (n.d.). Snort Users Manual Retrieved from Snort: http:www.snort.org
[46] Orbit-Computer Solution.Com (n.d.). Computer Training & CCNA Network Solutions Retrieved from : http://www.orbit-computer-solutions.com/Network-Security.php
[47] Cathayschool (n.d.) Intrusion Detection System Retrieved from: http://www.cathayschool.com/Intrusion-Detection-System-a1272.html
[48] Tech-faq. (n.d.). Network Attacks Retrieved from Tech-faq: http://www.tech-faq.com/network-attacks.html
[49] Botany.org. (n.d.). Mysterious Venus Flytrap Retrieved from Botany.org: http://botany.org/bsa/misc/carn.htmlwww.tech-faq.com/network-attacks.html