Network Security Management:

Solutions to Network Intrusion Related Problems

Agbogun, Joshua Babatunde.
Dept. of Mathematical Sciences,
Kogi State University,
Anyigba, Nigeria.
e-mail: ajbjoshua {at} gmail.com

Ejiga, Fredrick A.
Department of Statistics,
University of Ibadan,
Ibadan, Nigeria.

Abstract— **Systems and communications networks has grown increasingly over the years with a proportional increase in hacking software, studies and supportive forums that illegally encourage network intrusions. This paper presents the classes of intrusion, methods, tools and procedures intruders employ in accomplishing several networks attacks as well. Every class of intruders' attacks are motive variant and mission specific. However, this research presents recommendations on how attacks can be minimized and prevented from the backend system administrator as well as the front end user or client.**

Keywords-component; intrusiion; hacker; intruder; internal threats; external threats; session hijacking; repudiation; intrusion detection system; cyclic redundancy check; signature-based detection; IDS; CRC; attack; exploit.

I. INTRODUCTION

Information Systems and Networks are subject to electronic attacks. Attempts to breach information security are rising every day, along with the availability of the Vulnerability Assessment tools that are widely available on the Internet, for free, as well as for a commercial use. Tools such as SubSeven, BackOrifce, Nmap, L0ftCrack, can all be used to scan, identify, probe, and penetrate computer systems. Firewalls are put in place to prevent such unauthorized access to the Enterprise Networks however, the unanswered question is "can firewalls fully secure our systems and networks"?

The use of an Intrusion Prevention System (IPS) and/or Intrusion Detection System (IDS) can be very effective in preventing and/or detecting the exploitation of certain classes of vulnerability over the network. This is most commonly achieved by matching patterns against the raw bytes sent over the network. This approach can be improved upon by breaking the raw bytes into constituent parts also known as protocol fields before applying appropriate checks on the parsed data. The goal is to maximize both the confidence of the detection and the resilience of the IDS/IPS systems to evasion. Statistics shows that 25% cybercrime remain unresolved, 75 Million Scam Emails are sent every day claiming 200 victims. 73% of Americans have experienced some form of cybercrime and (65% globally) do the same, 10.5% of the world's Hackers from the UK, 66% are American and 7.5% are Nigerian of which Brazil suffers from more than any other country with 83% of the population having suffered from internet crime [1]

II. SYSTEM/NETWORK INTRUSION: HACKERS, CRACKERS AND INSIDERS EXPLOITS.

The most common usage of "hacker" is to breakdown computer security without authorization usually through a computer network or the internet for terrorism, vandalism, finance fraud, identity theft, intellectual property theft, and many other forms of crime. This can mean taking control of a remote computer through a network, or software cracking. These hackers are called crackers or black-hat hackers or simply "criminals". If on the other hand, an individual helps the government or special licensed organization to trace the intrusions of black-hat hacker and break (hack) the network of the criminals, such a person is called as "Ethical Hacker". Hackers have enormously more power available through the internet access, and they easily break network access by using user-friendly hacking tools."

A. Motives of black-hat hackers

The hacker motives are classified in three broad categories:

- Remuneration: Hackers of this class hack the network for personal gains which includes transfer of funds to their own bank accounts onshore or offshore, 'hackers for hire' who also break network on paid basis.
- Revenge: Dissatisfied customers, disgruntled former employees, angry competitors comes in this category.
- Recreation: Those who hack into network for 'just fun' or to prove their technical powers.

Hackers are very sophisticated in computer programming and have an endless amount of ways of bypassing a firewall to access a network and a Personal Computer (PC). Regardless of antivirus updates, a hacker can still find a way around the newest upgrades on antivirus programs and firewalls. A network intruder on the other hand gains unauthorized access to the networking devices through physical, system and remote attempts. The intruder uses some outdated exploits that are ineffective against up-to-date patched hosts. The intruders are of two types;

The first is the external intruder who is an unauthorized user of the system or network, while the internal intruder is an authorized user who has access to certain areas of the internal system or network. The intruders are basically of three forms one 'masquerade user' who is an authorized user of the computer, second 'misfeasor' who is a legitimate user that misuse his/her privileges and third 'clandestine user' who seize his supervisory control of the system and uses it to suppress audit information. [2]

B. *Motives of intruders*

The intruder's main motives are;

- To perform network scan to find out vulnerable hosts in the network.
- To install an File Transfer Protocol (FTP) server for distributing illegal content on network (e.g. pirated software or movies)
- To use the host as a spam relay to continuous flood in the network
- To establish a web server (non-privileged port) to be used for some phishing scam and not as an independent document. Please do not revise any of the current designations.

C. *How exploits are done*

- Scan for Vulnerable Systems: If you are a regular user of the modem in establishing Internet connection, a hacker can use what is known as a demon dialer to access your connection. This device redials thousands of phone numbers until it locates an open connection. On the other hand, if you are using a cable connection (i.e. Digital subscriber line) (DSL), the hacker can use a program that scans the IP address of your Internet connection or network to verify if the system is currently running. They can also use programs that spy on the information that is being transmitted from one device to another by using a "sniffing" program.
- Vulnerable IP Lists: Once hackers identify computers and networks vulnerable, they exchange lists of these addresses with fellow hackers after which a Trojan is loaded into the PC with the intention of snooping, spying, or destroying the computer's operating system. They additionally use a tool that system administrators use to test the security strength of a network system. The tool identifies vulnerabilities and provides the hacker with a list of exploits.
- Get Root: Once the hacker has accessed the network and gotten into the PC, the next step is to take over the PC operations. This is accomplished through computer programming commands that assist with searching the PC for the administrator password. After locating the password the hacker creates his own user account that is undetectable by the PC user and gains access to the programs and files on the PC.

This is one of the most common ways hackers gain access to a network and a PC. With all of the different ways that they can get access, it almost seems like your information and data will never be safe. This is true in the respect that with the ever changing world of technology new vulnerabilities arise with new computing systems.

III. CLASSIFICATON OF NETWORK THREATS

The Four Primary Types of Network Threats are:

- Unstructured threats
- Structured threats
- Internal threats
- External threats

A. *Unstructured Threats*

Unstructured threats often involve unfocused assaults on one or more network systems, by individuals with limited or developing skills. The systems being attacked and infected are probably unknown to the perpetrator. These attacks are often the result of people with limited integrity and too much time on their hands. Malicious intent might or might not exist, but there is always indifference to the resulting damage caused to others. The Internet has many sites where the curious can select program codes, such as a virus, worm, or Trojan horse, often with instructions that can be modified or redistributed. In all cases, these items are small programs written by humans. They aren't alive and they can't evolve spontaneously from nothing.

An individual launching an unstructured attack is often referred to as a script kiddy because he often lacks the skills to develop the threat themselves, but can pass it on anonymously and gain some perverse sense of satisfaction from the result. E-mail delivery methods have replaced "shared" game disks as the vehicle of choice for distributing this type of attack.

Unstructured attacks involving code that reproduces itself and mails a copy to everyone in the person's e-mail address book can easily circle the globe in a few hours, causing problems for networks and individuals all over the world. While the original intent might have been more thoughtless than malicious, the result can be a loss of user access while systems are being protected, a loss of reputation if the news that a company's site has been attacked, or a loss of user freedoms as more-restrictive policies and practices are implemented to defend against additional attacks. In some organizations, if the network is down, entire groups of people can't do their jobs, so they're either sent home or they sit and wait without pay because their income is tied to sales. So even if the hacker "thought" no one would be hurt, the result is often that they just beat some single parent or new hire out of a day's pay. Each of these results can be quantified in currency and often result in large numbers if and when the perpetrator is prosecuted. [3]

B. Structured Threats

Structured threats are more focused by one or more individuals with higher-level skills actively working to compromise a system. The targeted system could have been detected through some random search process, or it might have been selected specifically. The attackers are typically knowledgeable about network designs, security, access procedures, and hacking tools, and they have the ability to create scripts or applications to further their objectives.

Structured attacks are more likely to be motivated by something other than curiosity or showing off to one's peers. Greed, politics, racism (or any intolerance), or law enforcement (ironic) could all be motives behind the efforts. Crimes of all types where the payoff isn't directly tied to the attack, such as identity theft or credit card information theft, are also motivations. On the other hand, International terrorism and government-sponsored attacks on another country's computer infrastructure are becoming well documented. Systems of interest might include utilities, public safety, transportation systems, financial systems, or defense systems, which are all managed by large data systems, each with vulnerabilities. [3]

C. Internal Threat

Internal threats originate from individuals who have or have had authorized access to the network. This could be a disgruntled employee, an opportunistic employee, or an unhappy past employee whose access is still active. In the case of a past network employee, even if their account is gone, they could be using a compromised account or one they set up before leaving for just this purpose.

Many surveys and studies show that internal attacks can be significant in both the number and the size of any losses. If dishonest employees steal inventory or petty cash, or set up elaborate paper-invoicing schemes, why wouldn't they learn to use the computer systems to further their ambitions? With access to the right systems, a trusted employee can devastate an unsuspecting organization.

All too often, employers fail to prosecute this type of activity. The reasons range from fear of the activity becoming public knowledge to knowing that, quite often, record-keeping systems haven't been developed either to provide adequate evidence or to prove that the transactions, no matter how ludicrous, weren't authorized. Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as "3.5-inch disk drive". [3]

D. External Threats

External threats are threats from individuals outside the organization, often using the Internet or dial-up access. These attackers don't have authorized access to the systems. In trying to categorize a specific threat, the result could possibly be a combination of two or more threats. The attack might be structured from an external source, but a serious crime might have one or more compromised employees on the inside actively furthering the endeavor. [3] Figure 1 shows the recent trend of attacks while Figure 2 shows the distribution of targets while Table 1 shows the threats be categories.

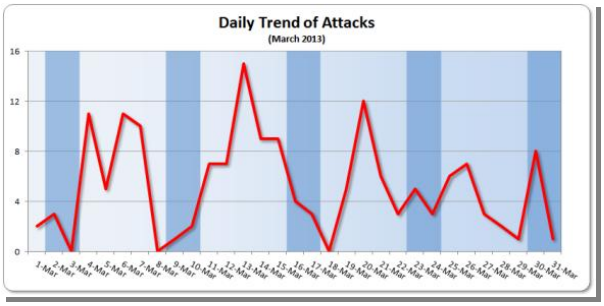

Figure 1. Daily Trends of Attacks [4]

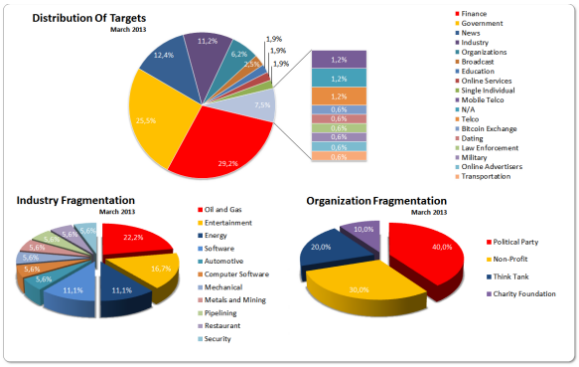

Figure 2. Distribution of Targets [4]

TABLE I. VULNERABILITY AND THREAT CATEGORIES [5]

	2010 Monthly Alert Numbers				2011 Monthly Alert Numbers				2012 Monthly Alert Numbers			
	Total	Reamp	New		Total	Reamp	New		Total	Reamp	New	
January	417	259	158	417	403	237	166	403	552	344	208	552
February	430	253	177	847	400	176	224	803	551	317	234	1103
March	518	324	194	1364	501	276	225	1304	487	238	249	1590
April	375	167	208	1740	475	229	246	1779	524	306	218	2114
May	322	174	148	2062	404	185	219	2183	586	343	243	2700
June	534	294	240	2596	472	221	251	2655	647	389	258	3347
July	422	210	212	3018	453	213	240	3108	514	277	237	3861
August	541	286	255	3559	474	226	248	3582	591	306	285	4452
September	357	167	190	3916	441	234	207	4023	572	330	242	5024
October	418	191	227	4334	558	314	244	4581	517	280	237	5541
November	476	252	224	4810	357	195	162	4938	375	175	200	5916
December	400	203	197	5210	363	178	185	5301	376	183	193	6292
	5210	2780	2430		5301	2684	2617		6292	3488	2804	

IV. NETWORK ATTACKS

While there are many variations and often different names, the four most common types of network attacks are

- Reconnaissance attacks
- Access attacks
- Denial-of-service attacks
- Data manipulation attacks

A. *Reconnaissance attacks*

The word "A reconnaissance attack, as the name implies, is the efforts of an unauthorized user to gain as much information about the network as possible before launching other more serious types of attacks. Quite often, the reconnaissance attack is implemented by using readily available information. Note that, employee names and e-mail addresses provide a good start in guessing the user name for an employee's account. Common practice is to use an employee's first initial and last name as the user name for their network computer account. E-mail addresses are also common user name for computer accounts. Large companies usually have their phone numbers assigned in blocks from the local telephone company, and many large corporations have their own dialing prefix. By using this information, the intruder can begin war dialing all the company phone numbers looking for a dial-up server. Once a dial-up server is found, the intruder can begin guessing account user names based on an employee's first initial and last name or their e-mail addresses. Brute force password crackers are freely available on the Internet. Once a user name has been guessed, it's only a matter of time before a weak password can be cracked. A war dialer is a program used to dial blocks of phone numbers until it finds a computer on the other end of the line. Once a computer is found, the war dialer application records the number dialed for later use by the intruder. [3][6]

To use a user account on a server or a network, you must first have the user name and password. Discovering the user names is a fairly straightforward process described in the preceding paragraph. Attackers use password crackers to crack the passwords to user accounts. Some password crackers find the encrypted password files on the server and decrypt them. When a hacker is unable to retrieve the password files, then brute force password crackers are used. Brute force password crackers attempt to log in to a computer account over and over, using multiple password combinations. Some cracking software uses dictionary files, while others attempt every combination of each key on the keyboard.

Knowing fully well that Internet Protocol (IP) address information is publicly available via the ARIN (American Registry for Internet Numbers) and many other Internet registering authorities. From www.arin.net, anyone can begin a search using a single known IP address. The search will yield the complete block of IP addresses belonging to the company. Domain Naming Systems (DNS) is another publicly available system that can provide a wealth of information regarding the IP addressing and naming strategies of virtually any company connected to the Internet.

For a company to host its own e-mail, web, ftp, or any other service on the Internet, it must first have each of these servers listed within the DNS infrastructure. These DNS servers list the names of the servers, along with the IP addresses that can be used to access these services. To mitigate these risks, security conscious companies could choose to host these servers and services outside their private networks with a hosting company. This added security is usually rendered obsolete, however, by adding backend connections from the hosting facilities back to their private networks.

B. *Access attacks*

The Access attack is a catch-all phrase to encompass a variety of forms of unauthorized access of computer resources. An access attack could be an outside individual, or a group that uses various methods to gain entry to a network and, from there, steals confidential information or engages in destruction of resources. An access attack could also be an inside (trusted) user getting into areas they aren't authorized to use. [3] Their intentions could be curiosity or the same as the outside hackers and these types of attacks can be further grouped into four categories:

- Gaining Initial Access: The first objective is to gain initial access, so additional reconnaissance can be conducted. This reconnaissance could include scouting out resources, IP addresses, and possibly running a network discovery (mapping) program or even a sniffer-type packet-capturing utility, hoping to capture administrative-level passwords. War dialers can be used to dial a large number of phone numbers looking for modems. A new variation involves sitting in a parking lot or in a building across the street with a laptop and a wireless network interface controller (NIC), looking for unsecured or poorly secured access points.
- Social Engineering: The term social engineering relative to security came from early hacking efforts on telephone systems and long distance services. Social engineering is based on the concept of why risk breaking into a system by brute force or tools when you can get some friendly employee to help you do it? Social engineering is generally a hacker's clever manipulation of an employee's natural human tendencies to trust and want to be helpful. More than one company with elaborate authentication processes, firewalls, virtual private networks (VPNs), and network monitoring software has been left wide open to an attack by an employee unwittingly giving away key information in an e-mail or by answering questions over the phone with someone they don't know. This is one area where the hacker can benefit from a friendly demeanor, a good smile, and knowledge of looking and acting like they belong.
- Password-Based Attacks: To use a user account on a server or network, you must first have the user name and password. Discovering the user names is a fairly straightforward process described in the preceding section. Attackers use password crackers to crack the passwords to user accounts. Some password crackers find the encrypted password files on the server and decrypt them. When a hacker is unable to retrieve the password files, then brute force password crackers are

used. Brute force password crackers attempt to log in to a computer account over and over using multiple password combinations. Some cracking software uses dictionary files, while others attempt every combination of each key on the keyboard, a time-consuming ordeal.

A good password system locks the account after a limited number of tries in order to thwart this type of attack. The successful hacker has the same access to resources as the users whose accounts they compromised to gain access to those resources. General password security lapses can put a password in the hands of an intruder. This can be as simple as passwords written on a desk pad, an appointment calendar, or an address book, to gaining access to a person's home or laptop computer where the logon password is being remembered by the OS.

One-time passwords (OTP) systems and/or cryptographic authentication can almost eliminate the threat of password attacks. OTPs involve using "what you have," such as password-token generator software on your computer and what "you know," such as a PIN number. The point here is that, the token software uses the PIN to generate what appears as a unique password. Once the token is used, it won't work again, thwarting the intruder with a sniffer product.

If standard passwords must be used, strong passwords (those that would be difficult to guess) can help. Strong passwords should be at least eight characters long and contain both uppercase and lowercase letters, numbers, and special characters (such as 35@!pQ*A). While randomly generated passwords might be the best, they're hard to remember and often lead users to write them down.

C. *Denial of Service attacks*

The Denial of service (DoS) attacks in their many forms is by far the most infamous, and possibly the most threatening to organizations who conduct any business over the Internet. The primary purpose of any DoS attack is to deny access to a device—or better, an entire network—by bombarding it with useless traffic. This attack has two ways to bury the target. First, the packets themselves can consume 100 percent of a device's resources, thereby preventing it from doing its regular work. Because a firewall or intrusion detection system could often easily defeat this type of attack. The second threat is that the organization's connection(s) to the Internet is filled to capacity with this useless traffic, thereby preventing in or out communications. For this reason, a DoS attack typically can only be defeated by the efforts of the organization's ISP. [3]

Because the ISP's upstream connection, called a fat pipe, is typically many times larger than the connection to each customer, the ISP might be completely oblivious to the attack. If the ISP's staff and service policies are less than optimal, the organization under attack might seem doomed. The true DoS attack launched by a single host generally isn't used, except by the least-experienced hackers. The two most devastating variations are the distributed denial of service (DDoS) and the distributed deflection denial of service (DRDoS). Both of these attacks enlist the assistance of others, often hundreds, of unsuspecting hosts to assist in the attack, thereby significantly increasing the size of the attack, further shielding the source, and making it harder to defend against.

- DDos: DDoS attacks start by the attacker(s) placing Zombie (technically, "bot," short for "robot") programs in a series of compromised computers hooked by relatively high-bandwidth connections to the Internet. These Zombies are programmed to monitor specific Internet Relay Chat (IRC) chat rooms to receive further instructions. The Zombie attack is directed and coordinated by a Zombie Master, who sends instructions to the individual Zombie, who then begins generating a flood of malicious traffic aimed at the target. Early DoS attacks on some famous web sites involved many computers on university campuses and even some from security agencies. These computers had unprotected security holes and they were online around the clock, and in addition provided large connections to the Internet. Today, DSL and cable modem connections make many home and small business computers more attractive as Zombie sites because they often lack the security features and staff to defend against the intrusion.

- DRDoS: The latest variation on the DoS, the DRDoS, involves one or more hosts sending a series of TCP SYN requests or ICMP (Internet Control Message Protocol) ping requests too many unsuspecting, even thoroughly secure, hosts using the "spoofed" source address of the target. When these hosts respond to what appears to be a legitimate, nonthreatening request, they collectively create an unsupportable flood of packets aimed at the target. Again, even if the target device(s) can determine what's happening, only a cooperative ISP can block the traffic before it buries the target's Internet connection. If the originating source continues to vary the type of packets sent to the reflectors, the filters at the ISP have only temporary or limited usefulness before they need to be changed.

While the threat of DoS attacks can't be eliminated, it can be reduced through the following three methods:

- Implementation of Anti-DoS features: Proper implementation and configuration of anti-DoS features available on routers and firewalls can help limit the effectiveness of an attack. These features could include limiting the number of half-open connections allowed at any given time or limiting the number of certain types that can originate from a source address.

- Implementation Anti spoofing features: Proper implementation and configuration of anti-spoofing features on routers and firewalls can help limit a hacker's ability to mask their identity. RFC 2827

filtering should be configured at a minimum (see the upcoming section "IP Spoofing").

iii. ISP traffic rate limiting: The ISP should agree to filtering limits on the amount of nonessential traffic that can cause cross link(s) to the company at a time. The filtering might limit the volume of ICMP traffic, a common source of distributed denial of service (DDoS) attacks, into a network because it's used only for diagnostic purposes.

D. Data manipulation attacks

The Data manipulation, or impersonation, is made possible by vulnerabilities in IP protocols and related applications. Data manipulation attacks are often called "man-in-the- middle" attacks because the attacks typically involve an individual located between TCP/IP-exploited IP vulnerabilities. [7] Common forms of these attacks include IP spoofing, session replay, session hijacking, rerouting, repudiation, and vandalizing web pages.

- IP Spoofing: An IP spoofing attack involves an external or internal hacker who pretends to be using a trusted computer by using the address of that computer. The hacker either uses an IP address within the range of trusted internal addresses for the network or an authorized external address that's both trusted and allowed access specified network resources. IP spoofing is often a tool used as part of other attacks, such as any variation of DoS attack, to hide the hacker's identity. IP spoofing is often limited to the introduction of malicious data or commands into an existing data stream in a peer-to-peer network session. Spoofing a source address might enable data to be sent through a router interface with filtering based on the source address.

  The threat of IP spoofing can be reduced, but not eliminated, through the following measures:

  a) RFC 2827 filtering: Basically, RFC 2827filtering means filtering out any IP addresses from coming into a network segment that should already be on that segment. If the entire 195.17.1.0 network is attached to a router interface, then no legitimate packets with source addresses in that network should be coming in through the router. This should be applied to edge routers for sure, but it can also be used on internal routers to prevent spoofing within the network. Similarly, limiting any outbound packets leaving the network to ones that have source addresses assigned to that network can prevent a network's hosts from spoofing other networks. This could be the result of an attacker on the inside or a DoS both on a local host participating in an attack on an outside host. If the company can get its ISP to perform RFC 2827 filtering on packets coming into the network, it would preserve the bandwidth of the link and kill some hack attempts. Spoofing could be virtually eliminated if all ISPs filtered client traffic allow only source addresses assigned to that client. If hackers can't spoof it, this makes going undetected harder

  b) RFC 1918 filtering: RFC 1918filtering means filtering out RFC-defined "private" addresses from entering or exiting the network segment. Because they have no business on the Internet, they shouldn't be there. If private addresses are used in the network, RFC 2827 filtering will include them.

  c) Change Non-IP address authentication: IP spoofing is worthwhile when devices use IP address–based authentication. If you use additional authentication methods, IP spoofing attacks lose much of their value. Cryptographic authentication is the strongest form of additional authentication, but if this isn't possible, use strong, two-factor authentication, such as One Time Password (OTP)..

- Non-IP address authentication: IP spoofing is worthwhile when devices use IP address–based authentication. If you use additional authentication methods, IP spoofing attacks lose much of their value. Cryptographic authentication is the strongest form of additional authentication, but if this isn't possible, use strong, two-factor authentication, such as One Time Password (OTP).

- Session Replay and Hijacking: Session replay is a form of a man-in-the-middle attack, where the intruder captures a packet sequence and modifies part of the data before forwarding it on normally. This type of attack relies on an inherent weakness in data traffic authentication. Session hijacking is a form of a man-in-the-middle attack where the attacker takes over an IP session that's underway by spoofing source and/or destination thereby addressing and altering TCP sequence numbering. Typically, a packet sniffer is used to set up the hijacking by allowing the user to see the existing traffic.

- Rerouting: Rerouting involves either gaining access to a router to change the route table entries, or spoofing the identity of routers or hosts so traffic is directed to a compromised device. Spoofing ARP replies is even possible. It causes a host to forward packets intended for a specific host or the default gateway to be forwarded instead to another local host. The new destination host can perform its assigned task and then forward the packet on to the correct destination.

- Repudiation: Repudiation is the denial of having been a part of a data exchange. This repudiation might be to avoid responsibility for an action. Nonrepudiation is a security feature that helps ensure that data has been sent and received by the parties claiming to have sent and received it. Nonrepudiation guarantees that the sender of a message can't later deny (repudiate) having sent the message. Similarly, the recipient can't deny having received the message. Methods for implementing nonrepudiation include the following:

a) Digital signatures: Unique identifier for an individual, much like a written signature.

b) Confirmation services: The message transfer agent creates digital receipts indicating messages were sent and/or received.

c) Timestamps: The date and time a document was composed, proving a document existed at a certain time

V. IMPROVING NETWORK SECURITY

A. Measures to Improve Network System

Here is a brief list of security measures to think about when installing a LAN:

- Virtual data physical security: This could mean keeping your server in a locked room, removing disk drives from workstations that don't need them, and installing an alarm system in your office.
- Beware of bugs: Most computer viruses are just nuisance, but it takes only one malevolent virus to bring your network to its knees. Install reliable antivirus software, keep it updated, and train your employees to use it. Think about other protective measures, such as installing only shrink-wrapped commercial software on your computers. Never think of installing cracked, patched or pirated software(s) because, they also provide open doors for attack.
- Daily Network Security updates: Stay on top of changes that could affect the security of your LAN. Keep your operating system updated with the latest security patches and bug fixes. Assign access to directories and other network resources on a need-to-have basis, and remove a user's account immediately when they leave your company. Use network logging and security tests to check your network for security holes and possible break-ins.
- Pay attention to passwords: Once a bad login is detected, the account should be suspended until the user complains of inability to log in to the network
- The image of the security wheel implies, network security is a constantly evolving and growing process. This process is driven by the changing and growing nature of the business on one side leading to more and more resources and possibly links to more outside sources. Pressing from another side is the bad minds outside your network who are constantly gathering better tools, often the same ones you'll be learning about. They also don't have a security policy preventing them from trying the latest and greatest hack posted on the Internet. They could also have "cracked" copies of licensed tools and software the company can't afford. If potential attacks from two growing fronts weren't bad enough, internal users are becoming savvier about the workings of the network. Economic turmoil can often bring out a side of people that even they might not have known existed under other circumstances.
- Planning and development must always look at the next level of safety the network security can be moved to. Meanwhile, caution and good practices would suggest the following:
- Monitor the security alerts from all network device vendors and install the recommended patches and upgrades.
- Stay current on the latest threats, vulnerabilities, and tools by monitoring security web sites and newsgroups, such as www.sans.org, www.cert.org and www.cisecurity.org.
- Implement and follow the existing network security policies, including incident investigation and reporting. Lax implementation and enforcement leads to potential vulnerabilities and can undermine commitment to security.
- Update the security policy on a regularly scheduled basis, plus any time a new technology is added to the network or an existing technology is removed.
- Ongoing security training and awareness should be a priority at all levels within the company.
- Encourage a sense of trust and friendliness to encourage employees to "ask first" when in doubt and to encourage reporting of potential security incidents.

There are a few things you can do to reduce the chances of a hacker intruding on your network and PC. In addition to implementing a solid antivirus program armed with a spyware, phishing, and adware detector you can also add a few other security components that will protect some of the vulnerabilities not covered by your antivirus program. These include an intrusion detection system and the latest security patches which will patch up any vulnerabilities or holes that currently exist in your network or PC's operating system.

B. Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station.[8] Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization. IDPSes typically record information related to observed

events, notify security administrators of important observed events, and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack's content.

For the purpose of dealing with Information Technology, there are three main types of IDS:

- Network intrusion detection system (NIDS): is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network intrusion detection systems gain access to network traffic by connecting to a network hub, network switch configured for port mirroring, or network tap. In a NIDS, sensors are located at choke points in the network to be monitored, often in the demilitarized zone (DMZ) or at network borders. Sensors capture all network traffic and analyze the content of individual packets for malicious traffic. An example of a NIDS is Snort.
- Host-based intrusion detection system (HIDS): It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file system modifications (binaries, password files, capability databases, Access control lists, etc.) and other host activities and state [9], [10]. In a HIDS, sensors usually consist of a software agent. Some application-based IDS are also part of this category. This was the first type of intrusion detection software to have been designed, with the original target system being the mainframe computer where outside interaction was infrequent [11] Examples of HIDS are Tripwire and OSSEC.
- Stack-based intrusion detection system (SIDS): This type of system consists of an evolution to the HIDS systems. The packets are examined as they go through the TCP/IP stack and, therefore, it is not necessary for them to work with the network interface in promiscuous mode. This fact makes its implementation to be dependent on the Operating System that is being used.

Though they both relate to network security, an intrusion detection system (IDS) differs from a firewall in that, a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. This is traditionally achieved by examining network communications, identifying heuristics and patterns of common computer attacks, and taking action to alert operators. A system that terminates connections is called an intrusion prevention system, and is another form of an application layer firewall.

Noise can severely limit an Intrusion detection system's effectiveness. Bad packets generated from software bugs, corrupt DNS data, and local packets that escaped can create a significantly high false-alarm rate.[12]

It is not uncommon for the number of real attacks to be far below the false-alarm rate. Real attacks are often so far below the false-alarm rate that they are often missed and ignored.[12]

Many attacks are geared for specific versions of software that are usually outdated. A constantly changing library of signatures is needed to mitigate threats. Outdated signature databases can leave the IDS vulnerable to new strategies. [12]

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS) are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. [8]

Intrusion prevention systems are considered as extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. [12] [13] More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. [14] An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options. [13][15]

Intrusion prevention systems can be classified into four different types: [8][16]

a) Network-based intrusion prevention system (NIPS): monitors the entire network for suspicious traffic by analyzing protocol activity.

b) Wireless intrusion prevention systems (WIPS): monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.

c) Network behavior analysis (NBA): examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations.

d) Host-based intrusion prevention system (HIPS): an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

The majority of intrusion prevention systems utilize one of three detection methods: signature-based, statistical anomaly-based and stateful protocol analysis. [12][17]

- Signature-Based Detection: This method of detection utilizes signatures, which are attack patterns that are preconfigured and predetermined. A signature-based intrusion prevention system monitors the network traffic for matches to these signatures. Once a match is found the intrusion prevention system takes the appropriate action. Signatures can be exploit-based or vulnerability-based. Exploit-based signatures analyze patterns appearing in exploits being protected against, while vulnerability-based signatures analyze vulnerabilities in a program, its execution, and conditions needed to exploit said vulnerability.
- Statistical anomaly-based detection: This method of detection baselines performance of average network traffic conditions. After a baseline is created, the system intermittently samples network traffic, using statistical analysis to compare the sample to the set baseline. If the activity is outside the baseline parameters, the intrusion prevention system takes the appropriate action.
- Stateful Protocol Analysis Detection: This method identifies deviations of protocol states by comparing observed events with "predetermined profiles of generally accepted definitions of benign activity."[12]

VI. Conclusion and Recomendation

This paper was able to identify various forms of network attacks, define the objectives of intruders as well as the process of executing their attacks. The study also presented several measures to limit and avoid future attacks by intruders into the network system.

Apart from the recommendations previously provided, any of the following applications amongst others can also be purchased provided, their features [18], [19], [20] which will also be listed suits your network. Cisco Intrusion Prevention System [21], IBM Security Network Intrusion Prevention System [22] as well as Stone Gate Intrusion Prevention System [20] all with solutions that accurately identify, classify, and stop malicious traffic, including worms, spyware, adware, network viruses, and application abuse, before they affect networks and systems.

References

[1] [1] Cyber Crime Statistics: http://www.cybercrimeswatch.com/cyber-crime/cyber-crime-statistics.html

[2] Sushant, M. (2012) Hackers & Intruders: Motives and Difference. International Journal of Engineering and Computer Science Engineering 1(3). Pp1446-1448

[3] http://ptgmedia.pearsoncmg.com/images/1587131625/samplechapter/1587131625content.pdf

[4] http://hackmageddon.com/2013-cyber-attacks-timeline-master-index/

[5] https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf

[6] http://www.orbit-computer-solutions.com/Types-of-Network-Attacks.php

[7] http://www.sans.org/reading_room/whitepapers/application/approach-application-security_16

[8] NIST – Guide to Intrusion Detection and Prevention Systems (IDPS). 2007http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[9] C. Kerry; G. Christopher, Managing security with Snort and IDS tools (O'Reilly Series. O'Reilly Media, Inc, 2004)

[10] M.C. Duffy, The 10 dumbest mistakes network managers make, InfoWorld (IDG Network),2009,http://www.infoworld.com/d/security-central/10-dumbest-mistakes-network-managers-make-162?page=0,2&r=974, retrieved 2011-07-31

[11] Debar, Hervé; Dacier, Marc; Wespi, Andreas . "Towards taxonomy of intrusion-detection systems". Computer Networks31 (8): 805–822. doi:10.1016/S1389-1286(98)00017-6.

[12] M. E. Whitman; H. J. Mattord, Principles of Information Security. Cengage Learning EMEA, 2009, 289.

[13] R. C. Newman, Computer Security: Protecting Digital Resources. Jones & Bartlett Learning, 2010, 273

[14] T. Boyles, CCNA Security Study Guide: Exam 640-553. John Wiley and Sons, 2010, 249–280.

[15] H. F. Tipton; M.I. Krause, Information Security Management Handbook. CRC Press. 2007, 1000 -

[16] J. R. Vacca (2010). Managing Information Security. Syngress. 2010, 137

[17] E. Kirda, S. Jha; D.Balzarotti, Recent Advances in Intrusion Detection: 12th International Symposium, RAID 2009, Saint-Malo, France, September 23–25, 2009, Proceedings. Springer. pp. 162

[18] Cisco ASA 5500 Series Adaptive Security Appliances: http://www.cisco.com/go/asa

[19] IBM Security Network Intrusion Prevention System

[20] Stone Gate Intrusion Prevention System (IPS) Solutions: http://www.stonesoft.com/en/products /ips /

[21] Cisco SDM, http://www.cisco.com/en/US/products/sw/secursw /ps5318/index.html

[22] http://www-01.ibm.com/software/tivoli/products/security-network-intrusion-prevention/