INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Foundation of Information Assurance
NEXT GENERATION INTRUSION PREVENTION SYSTEM

Sarvesh Kapre

Master of Science in Information Assurance
College of Computer and Information Science
Northeastern University, Boston, Massachusetts
kapre.s@husky.neu.edu

Abstract: *Security is a field which is analogous to a game of chess. The different security layers are just like the pawns; once lost, the king is exposed. Here the king represents information in a system, thus reflecting a security breach. The key here is to understand the game by anticipating the movements and create a barrier to prevent intrusion. Today, where viruses, worms, hackers, Trojans and malwares are running rampant, we must design a full proof intrusion prevention system to play a role in protection of the king. In the field of network security, constant prudence is a fundamental requirement. Even a single negligence can prove catastrophic, the security engineers must be on their toes and safeguard the vital information of masses. The need for intrusion prevention system arose from the fact that most of the technologies such as the firewalls, intrusion detection systems, secure web browsers etc. have some loop holes, when exploited, allow the traffic to move unfiltered through them. In this paper, we shall discuss in detail the different technologies involved in next generation intrusion prevention system, their functionality, effectiveness and performance which enhances the level of security involved in network infrastructures of organizations as well as the home networks.*

Keywords*: Intrusion Prevention System, TCP Sequencing, Zero Day Attacks, False Positives, Buffer Overflow, Adaptive Security, Threat Landscape, DDoS attack, Signature Matching, Drive-by-Download.*

1. INTRODUCTION

Defense in depth is a very comprehensive security strategy which contains different layers of protection, where each layer filters the traffic which proceeds to the next layer where it is again scrutinized. Obtaining a complete security is next to impossible; because, you need to bypass some traffic in-order to allow communication between the systems via network. This in return, provides an opportunity for the attackers to compromise a network. To prevent this unwanted intrusion, we add different layers and different technologies which resists the progress of attacker intruding the system.[1] Technology which we use is the Intrusion Prevention System (IPS). IPS sounds similar to Intrusion Detection Systems (IDS) and even few methodologies involved in both these technologies are the same; but, the major difference lies here is in the name itself, that is; "detection" and "prevention". IDS only alarm the network administrators about the intrusions taking place in the network. IPS is a network security and threat management system which is placed behind the firewall and in-line with the communication path between source and destination to block unwanted traffic, drop malicious packets prevent attacks by taking suitable action. First let us understand the difference between a firewall and an IPS. Firewall has number of rules imbibed in it, maybe ten, maybe hundred or maybe even thousands of rules and all these rules are "allow" rules where the firewall allow the traffic to enter in the network once it has reached the bottom of the stack after checking for each rule. An IPS is exactly the vice-versa of firewall. Even it has hundreds or maybe thousands or maybe even lakhs of rules imbibed in it, but all these rules are "deny" thus making sure that the known type of threat packet is not entered into the system. As the packet is entered, its content is check down the stack of IPS and if the content is matched the packet is denied from entering. So IPS is normally termed as control devices. So, if you are a pen tester and using popular exploit tool to find and discover new attacks, you probably have a decent time window to find out a new exploit and add that patch in the IPS thus making it capable of handling new attacks.[2] Just as IPS is a control tool, IDS is a visibility tool. If we compare an IPS to a firewalls, then we can compare and IDS to a protocol analyzer. The basic job of the IDS to sit on the network and monitor the traffic at different point, thus providing scanned info of what is happening inside a network to a network administrator. So for a network administrator we can call it a window to peep out to watch some traffic flowing in the network. Just like an IPS it also provides info regarding security policy violations, viruses or malwares, information leakage, or any unauthorized clients trying to get entry into the system. Both these tools are valuable, as IPS will block intrusion and IDS will detect intrusions, but they do much more than these tasks. So the question is, which one to buy, if both are equally good? Answer is IPS. The simple reason and logic behind this is that IDS can only detect the traffic and cannot block it. With the workload on staff increasing day by day, the deadlines getting tighter and tighter, with the advent of fast paced life, no one has time to sit and watch the traffic flowing through the network. Someone must be there to act and that is the job done by IPS, by preventing the entry. This created the need for vendors to enhance IDS systems to make them work as IPSs.

Part I. Contextual analysis of network behavior and its implementation

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

1. Analysis of the network

It is important from contextual analysis point of view to understand the topology of the network. It is equally important to understand the known hosts as well as the new hosts, the configuration changes in the host and network architecture and the policies developed by the IT department. In-order for the IPS to determine the addition of new host onto the network where it is place, it must monitor the network continuously. Today's network is highly dynamic and the threats and vulnerabilities evolve continuously. The attacks are becoming more and more sophisticated and as a result static defense which were a part of traditional IPS are becoming obsolete and this is the age of implementing dynamic security for the dynamic world. The real-time network analysis complements the intelligent automation process as it involves vulnerability assessment of the target using different technologies, analyzing the network flow, and discovery of the network passively.[13] The awareness of network helps the organization to protect their network in the following ways.

- Enforcing and monitoring the compliance of the network.
- Tuning and maintaining an IPS by reducing the workload across the network.
- Detecting the traffic anomalies and changes in the configuration of network.

2. APPLICATION TESTING AND ANALYSIS

The next generation IPS automatically performs testing and analysis of the applications deployed on the network with the tools installed in it. This is important because the vulnerabilities in the applications can be easily identified by the remote hackers using vulnerability assessment tools and these vulnerabilities can be easily exploited thus gaining remote access into the network. The vulnerabilities within these applications must be known to the IPS and the suitable policies must be developed and updated in the IPS. The next generation IPS performs comprehensive analysis of the software built within the organization as well as the purchased third-party applications. Thus, the financial profit for the company is that, they need not buy any expensive application testing tools to perform vulnerability analysis of the applications deployed on the network as the next generation IPS is very capable in doing the same.[14]

3. IDENTITY ANALYSIS

This feature of the next generation IPS is the most favorite for any network administrator. This is due to the following reasons:

i. Visibility of the user activity is increased.

- It manages the user access to the network and system resources and applications centrally.
- Enforcement of the policy as that created by the network administrator.
- It can easily distinguish between users and guest and even identify some entity which is not categorized as user or guest.

ii. Control of the corporate resources is improved.

- The users can work remotely but it prevents the access or use of any unauthorized resources or even the sites which are banned by the corporate policies.
- The data loss can be prevented and the threats can be reduced as there are restrictions placed on the use of resources for the users who are accessing them remotely.
- According to the machines and locations the users are granted granular access to the data centers, segments of the network and application.

iii. Effective and easy deployment of next generation IPS.

- The network administrators can choose between various deployment option such as identity agent, captive portal or clientless with flawless active directory (AD) integration. Thus it is completely transparent to the users.
- Captive portal helps in identifying and authenticating the user through a web interface and after verifying their credentials access can be granted to the corporate resources on the Intranet. Here, if the user is authenticated then without any further screening, he is redirected to the network but a failed identification even once, redirects the user to captive portal where he needs to enter his credentials. This feature prevents the attacker from brute-forcing his way into the network.[15]
- The endpoint identity agents help in the prevention of illegitimate entities on the network by identifying the machine names and users (Kerberos based).
- Only the network or system administrators can modify or edit the necessary configurations. As a result of this, the user intervention is minimized.
- IP spoofing is prevented with the use of packet tagging technology.

4. BEHAVIOR ANALYSIS

Most of the techniques in IPS involves; "allow" or "deny" rules. The simple logic behind these techniques is creating a list of services or packets or users and classifying these legitimates entities in whitelist and the rest of doubtful or threatening entities in blacklist. So, the next question which pops us is; what is blacklist and whitelist and are they sufficient to guard us from the attackers? What else does the next generation IPS add to increase the security? The answer is, in next generation IPS assign's one more layer of authentication is added which is based on behavior of the entities. The logic behind this is simple and applied in day-to-day life. For example: airport security system has a database containing the list of the information of people who are to be denied such as terrorists or criminals. So this is basically a blacklist and the people in this list are denied from any further access. Some people have gained a tag of good citizens and are granted permission after performing all background checks. The people contained in this list are allowed access without authentication. This is nothing but a

whitelist. Normal people, who purchase a ticket, have to undergo security checks, to granted access to fly. A trained law enforcement person carefully analyze the behavior of these people and if they are found behaving in suspected manner, are prohibited from going further. This is nothing but behavioral analysis. The same, simple logic explained above is used while whitelisting, blacklisting or behavioral analysis of packets or users or any other entities trying to gain access in the system.[11]

5. POWERED BY SNORT

- **Increased accuracy**: Snort community incessantly updates its database and the source code of Snort with new threats, attacks and malwares being introduced daily round the globe. This naturally benefits the IPS even without the network administrators needed to do a thing apart from updating and patching the Snort.
- **Expeditious response**: The network administrators can protect their infrastructure by customizing the rule database of Snort, adding new rules confine to their own network and related policies. When policies and set of rules defined in the IPS complements each other, the productivity is increased to a greater extent.
- **High adaptability**: As it has an open architecture where we can view, edit and create our own rules. We have access to its source code and documentation which helps in designing our own functions and adding it to Snort, which will help us in creating a unique set of network solutions designed only for own enterprise.
- **Data-leak prevention**: This is a built-in feature of Snort which helps in analysis and identification of illegitimate activities going out from the internal network to external network such as transmission of sensitive data through unauthorized methods which includes social security numbers, credit card infrastructure, confidential documents of projects, employee details working in the company etc.
- **Network and host information**: Evaluation of the hosts and network data can help the network and system administrators to speed up the response activities in case of a security event. The next generations IPS gathers the network logs for each system and also back-up these logs in case of any failure. This information is presented in user friendly format which helps to spot on the problem of any particular system immediately.
- **Keeping track of user activities**: It is said that; the most vital threat to any organization are its employees, as they have the direct access to the systems and the information within it such as a database. Hence, it is important to track the user activities, inside the network of an organization, so as to identify any illegitimate activities. Next generation IPS also warns the network or system administrator, if any user has purposefully or accidentally deactivated their anti-virus protection, by providing the corresponding employee name and system number. The tracked user information and activity, also helps to speed up an investigation of any incident or case in an organization. The next generation IPS, sends automated alerts to particular user, if they have not upgraded or updated their antivirus, adding further protective security measures.

Part II. Basic techniques

1. URL filtering.

As IPS is a control device which is based on “deny” rules; URL filtering is the major technique used here. The main technique of URL filtering lies in customizing the white-list and black-list. White-list provides the list of legitimate packets which will be granted access without any resistance and black list will discard the packets contained in its list. Though, professional attackers gain entry into the system by disguising the packets as some legitimate entity and by encrypting them using white-list, this technique at-least minimizes the probability of getting attacked. By specifying the permitted website which can be visited, we can prevent unwanted, videos, images, or content. Providing additional security can block the spyware and malware thus reducing the administrative overhead in keeping the system clean. It also provides the list of websites visited by any individual on that particular network and provide us the data of incoming and outgoing packets along with the used bandwidth which helps in identifying inappropriate use. Network administrators can also set the time during which the internet can be accessed. List of websites to be blocked is created by looking at current threats and analyzing the history of previous attacks from the services, and then by blocking this list. Guest users are put under various restrictions while using LAN, while the local users are given much more privileges. Active Directory helps in building policies for users and groups and then a report can be prepared after few months to find out how effective this policy has been. URL filtering is modified on the next-generation IPS in such a way; that, if there is excessive incoming traffic on a particular network, that port can be blocked or shut down temporarily or by diverting the traffic to the remote system to check for authentication by the system administrator. This will prevent brute-force attack and even if the packets are legitimate they can be re-diverted back to that port and then allowed access. It maximizes the performance and flexibility by using on-box database containing URL which is enabled using local lookups. The URL filtering can be customized by the network administrators to enhance the employee experience and at the same time providing security. The SSL decryption policies are enabled so as to allow encrypted access to particular websites which are harmless and visited by the employee’s like finance, health and shopping and decrypting the traffic to all other websites like social networking, blogs, forums and other entertainment sites. In IPS few results or searches are classified as cached results. Whenever, any user tries to visit the cached results of internet explorer or google search, URL filtering policies are applied. This prevents the download and uploads for the defined URL address in the cached results which represents high risks. To prevent any illegitimate content to appear in the users search engine, safe search is enabled and only the allowed content defined in

the policies set by the network administrator can be viewed and the rest results are blocked.[4]

2. Distinguishing false-positives.

There must also be a frequent update of this IPS to tell the recent virus updates and providing input on malicious and non-malicious activities to improve this system. The inspection agent is programmed to perform prevention activities by following particular steps in the same order as instructed. The parameters can be customized by inspection agent by performing context-sensitive fingerprints on specified application so as to prevent the number of false-positives.[7] Database containing variety of system fingerprints for known vulnerabilities and exploits is maintained in the IPS and then traffic matching is performed to check for false positives. The fingerprint update on IPS must be regularly provided for keeping the system up-to-date. Hybrid adaptive next generation IPS uses a combination of powerful detection method and intelligent event correlation.

3. Data-loss prevention

The job of Intrusion Prevention Systems is to prevent the system from attacks. But what is the use of implementing the technology of Data Loss Prevention (DLP) in next generation IPS? Preventing data loss is the best way to avoid the damage, loss private or proprietary information and potential breach, thus maintaining the confidentiality, integrity and availability of information. DLP helps the system in identifying the systems and technologies that are designed to cause the data breach in a system by exploiting the vulnerability and trying to extract the data from the safe storage or by gaining access to the database where vital information is stored. Thus the DLP devices triggers the prevention of data loss by monitoring, detecting and then blocking access to any sensitive data and information in the enterprise.[17]

The protection mechanism implemented by DLP consists of three methods:

- **In-use protection**: The sensitive data of the organization is placed in a repository which can be accessed only by particular employees who have been granted access by sharing passwords or through access-control list. Such data remains in the encrypted form when not in use, thus it prevents any attempt in accessing the data and clicking snapshots of the same will give no plain-texts.
- **In-motion protection**: The data which is in motion is encrypted so as to protect it during transmission and minimize the risk of eavesdropping. More vital the data, stronger the encryption.
- **At-rest protection**: The access to the data stored on hard-disk is granted using access control list only to the particular legitimate employees. The data is monitored throughout and logs of the data accessed by the employees are maintained. Further, encryption is used in-order to guard the data from attacks.

The next generation IPS has inherited the quality of DLP; that is, to monitor and control the incoming and outgoing information, so as to safeguard the network. The DLP is one of the reasons for increased protection in the next generation IPS. There are three categories of DLP's: enterprise, channel and DLP-lite. The next generation IPS contains enterprise DLP. The enterprise DLP installs agents that scan the data repository, monitors the network traffic on the host and provides a full-suite of context aware monitoring and detection. These functionalities enables the IPS to block file transfer activity at host and withdraws the power of user to surreptitiously add data using external devices such as hard-disk, pen-drives etc.[8] DLP sniffs the network packets and reject the "bad traffic" depending upon the policy set-up by the organization. The main advantage of DLP is; it warns the user if they are trying to copy any unapproved file, thus setting restrictions and controlling the activities the in-house users can perform. The ability to sniff the packets, block unwanted data and prevent users from illegal actions on the host is what made the DLP a part of next generation IPS. The DLP must operate in an information processing environment which is defined by the security policies, for its proper and effective functioning. To verify that the threats to security, privacy and confidentiality are managed properly, regular auditing must be performed. Thus, in-short the overall idea for DLP is to watch out for attacks on the organizations sensitive data and taking appropriate preventive measures and implementing defensive strategies to safeguard the data.

Part III. Advanced techniques

Initial IPS system was capable of providing security. But, as the time progressed, even the attackers got matured enough and started exploiting the loop-holes in IPS, thus helping them in compromising a system. The need for the technologies such as: network behavior analysis, application monitoring, user identity tracking, host profile and network map, automated impact assessment, automated tuning, SIEM and data loss technology increased and this resulted in adding advanced technologies leading to the development of next generation IPS. The advanced techniques used in IPS are mentioned below-

1. Access control decision

To reduce the number of false positives, the next-generation IPS uses various methods for filtering. One of the methods is access control, which depends on the policy based detections, to prevent an attack on the system. The access control list contains a list of commands to which the corresponding action can be taken; like, deny or allow. As per the history of attacks and threats, it already contains built-in commands and functions to provide safe operation of system. But this policy mechanism must be evaluated and expanded frequently, to provide real-time security and safeguard against current attacks and threats. Before the "allow" permission is granted the packet has to go through various stages of authorization to check for its legitimacy.

There are four basic steps that the access control decision follows.[9]

- **Pre-conditions**: To gain entry, specify the true condition.
- **Request-result conditions**: Depending on the request accepted or denied, this condition must be activated.
- **Mid-conditions**: During execution of the requested operation, it specifies the true condition.
- **Post-condition**: After completion of the operation specify what must be true. This will trigger another activity such as logging and notifying whether the operation is successful or it fails.

2. Application inspection.

Security appliances on the network interface performs the inspection of packets passing through the network to check for its legitimacy. Several inspections are involved in this task and one type of inspection used in IPS, is the application inspection. This requires a modular policy framework, in-order to perform inspection activities such as traffic identification, inspecting the traffic and then applying inspections of this traffic. The next generation IPS not only scans and inspects the traffic but also memorizes the common traffic information which flows on a daily basis. Applications that need the source address to match with the IP address embedded in the packet requires the activation of application inspection. If a service is using dynamically assigned ports, the application inspection will monitor the session and permit exchange of information through those ports. The configuration in application inspection protocol involves a default policy which performs inspection on all the interfaces. We can also delete these default policies and create a new one, with more strict rules and exhaustive inspection, as per required on some active and less active ports.

3. Threat management

Threat management deals in providing real-time solution to the threats, by analyzing it and reacting with an accelerated incident response. Threat management in next-generation IPS provides us with a deeper insight into the network malicious traffic depending upon the policies, increased flexibility in dealing with the networks and maximizing the acceleration of the reaction time by performing actionable intelligence. The next generation IPS provides centralized management architecture with the storage of history of attacks, policies and recent threats. The threat management correlates between intrusions, files, malwares, connections, and discovery of new threats. It takes into account different conditions such as; host name of devices, different clients and servers connected in the network topology, intrusion policies, file policies, network discovery policies, access control policies, customized intrusion rules, activated custom fingerprints, whitelists, black lists and vulnerability database. The correlation between these policies and tools helps in minimizing the risks, packet loss and downtime, increasing efficiency in threat detection and increasing the capacity of data center to accommodate data. But, due to the rapid movement of traffic on the network, it is possible that some packets enter unchecked. Hence next-generation IPS consists of two threat management system interconnected with each other using a same user account and centralized data storage. As a result of their connection between them, these threat management systems complement each other and provide safe output. The threat management system increased the IPS availability, zero-downtime, flow survivability, expected asymmetric packet flows and elastic scaling.[10]

4. Custom IPS signature

Every company has a different network topology, different policies, different applications and different environment in which it functions. A default IPS cannot guard the network with its default policies and default content in the database. These policies and the content in it must be manipulated as per requirement of the network. Next generation IPS allows building and designing, our own signatures from allowing or denying any access entry into the network. You can design these signatures depending on the vulnerabilities existing in the network.

Thus, for customizing these signatures, following steps must be included –

a) Researching and identifying latest vulnerabilities.

b) Developing the necessary signatures.

c) Testing these signatures by performing ethical hacking.

The IPS can be customized as per requirement and the signature engine used in it can display the traffic entering the network to the security engineers to inspect its legitimacy. This features also helps us to keep the track of packets flowing through our network.

Can we term next generation IPS as an anti-virus?

The above mentioned tasks performed by the next generation IPS are similar to that of an anti-virus. An anti-virus provides a broad-based protection against a range of attacks which are well defined in its software configuration. The next generation IPS blocks worms, Trojan horse, viruses, botnet, spyware etc. Apart from this, it also guards the network from wide range of threats that includes:

- Policies that prevent the entry of malicious java-script and HTML to enter into the enterprise network.
- IPS is placed inline to the network which promotes stream-based protection against files which contains malwares inserted into it.
- Some files contain ransomware malware crypto-wall which has its payload written in java-script which tries to enter by disguising itself as white-list content. Even such files are denied access.
- It also leverages SSL decryption as explaining in URL filtering concept which block virus imbibed in the SSL traffic.
- Signature based filtering capability creates a database of known signatures and hybrid approach helps in the automated entry of newly recognized signatures in the database which helps in preventing against known and unknown attacks. In traditional anti-virus the new signatures are updated into the database by manually updating the anti-virus on daily basis.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

- Next generation IPS stores the files infected with malicious programs like virus, worms, Trojan horse in a separate isolated section, just like an anti-virus stores the infected files in a virus vault.
- Integrating it with Snort community provides continual updates of latest malware, threats and vulnerabilities which keeps the software up-to-date and blocking the latest illegitimate traffic.
- Drive-by-downloading occurs when a user visits a particular website and from there, the user is redirected to some other website which is illegitimate and triggers automatic download of an infected file without the consent of user. But the next generation IPS prevents drive-by-download.

Part IV. Implementation of hybrid adaptive approach in IPS

Chapter A. Introduction to hybrid adaptive approach

1. FLIPS (Feedback Learning IPS)

The feedback learning IPS is the new hybrid approach of the next generation IPS which consist of three main methods: signature-based filtering, anomaly based classifier and instruction set randomization. In-order to protect from binary code injection attacks FLIPS hybrid approach is used. This approach not only prevents this attack, but also stores the code injected in this attack. FLIPS stores the injected code and creates signatures which acts as a classifier in identifying and preventing the zero-day exploits.[20]

The main advantage of FLIPS is that, it does not require any existing content in the database to take any necessary action; it can react to a new attack and act accordingly by allowing or denying the service. FLIPS have two main components: Proxy and application supervision framework. The goal of this design is to deploy the system at single host. Whenever in packets are received from the input source, they are initially transmitted through the proxy. The dichotomous design of proxy consist of two core components: The signature filter and anomaly filter. The packet is initially check for matching signature and if the match is made, packet is dropped, as IPS is a control device. If no matching corresponding signature is identifies, it is filtered through the anomaly filter, where behavior of the packet is scanned. If the behavior of packet is abnormal, it is copied to cache. This is done in-order to avoid false positives. So, till now, only those packets are dropped whose signatures are matched and the rest packets are forwarded to cache. The function of application supervision framework is prevent a vulnerability from getting exploited, report it to the network administrators, make a corresponding entry into the signature database for the illegitimate packet so as to drop it in step one if it tries to re-enter again and the patch the vulnerability exploited or design policy to prevent the vulnerability from getting exploited again. The protected application and supervision framework with feedback mechanism are deployed within the firewall. The application framework identifies for the code injection attacks. The code is extracted and the feedback with code is provided to signature database in the proxy. The proxy is written in Java and contains PayL (400 lines of code), the supervision framework is provided by STEM (19000 lines of code), HTTP proxy that contains the signature matching filter is a 5000 lines code [20]. Whenever the packet enters the anomaly based classifier stage, PayL allocates a score to it. The first filter is signature and the second filter contains the score stored into it which was allocated by PayL. The longest common substring algorithm identifies the malicious traffic. Once the malicious traffic is detected, the second filter passes it back to the proxy for updating into its signature database.[20]

Chapter B. Main components of hybrid approach

1. Signature-based filtering

Known information of the traffic can be added to a database and the incoming traffic can be compared with its content and the necessary action can be taken to “allow” or “deny” it. But what about a new packet whose information is not present in the database and what action is taken by the next generation IPS on it? For this signature base filtering is done where the characteristics of the packet; for example, the information, pattern, texture, size and content is checked with the data present in the database. Depending upon the rules necessary action is taken. This change in the behavior of the packet is checked with the help of heuristic approach, which is quiet common in the firewall. When the new packet is allowed access it is automatically updated in a database, so that the same pattern can skip the necessary security checks to gain entry into the systems network.

2. Anomaly based classifier

Zero-day attack, which exploits the vulnerability in the software and which is unknown to the vendor, can be prevented to some extent, by comparing its pattern with the existing signatures in our database. But what about the new attacks whose behavior and pattern is totally different as that of the existing signatures and cannot be compared? Here the next generation IPS uses the behavior based detection by analysis different characteristics of packets such as rate of transfer of packets, movement of packet after entering the network and taking into account a source of a packet. So how does this work? The IPS contains the database of applications running on to the network. This database must contain all the applications and its interaction on the network. It is possible that few application might not have been in use since many year and whose vulnerabilities have never been exploited, even such applications must be a part of this database.

A table is created containing the following details such as:

Session rate - A threshold is set while establishing a session, and if the rate crosses this threshold, a network anomaly is triggered.

For example; if a threshold value of 500 is set on a TCP port than any connection resulting in 500 plus connections/second will result in an anomaly and will trigger a network alarm.

Suspected session rate - A network alarm will be triggered if the rate of unidentified network traffic, undetected by the

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

network crosses a certain threshold. This parameter works in conjunction with the Session rate.

Calculating the ratio - Ratio between the suspected session rates and session rates is calculated and then the necessary action is performed. A high ratio naturally corresponds to a high level of unresponsive sessions occurring on the network.[12]

Table 1: Distinguishing between IPS and next generation IPS

Features	IPS	Next generation IPS
IPS Detection and Blocking	YES	YES
Centralized Event data	YES	YES
Reports, Alerts and Dashboard	YES	YES
Third-Party Integration	YES	YES
Policy Management	YES	YES
Pre-packaged hardware	YES	YES
Cisco Supported	YES	YES
Network Behavior Analysis	NO	YES
Application Monitoring	NO	YES
User Identity Tracking	NO	YES
Host Profile and Network Map	NO	YES
Automated Impact Assessment	NO	YES
Automated Tuning	NO	YES
Interface Modularity	YES	YES
Scalability and Flexibility	YES	YES
Up to 20 Gbps IPS Inspection	YES	YES
SIEM	NO	YES
Data Loss Prevention Technology	NO	YES

3. Instruction set randomization

One of the most common method used by an attacker in-order to compromise a network is the use of code injection attacks. In-order to perform this attack, the attacker must identify the instruction set and then inject malicious code in it, to gain a user privilege. Even if the attacker is able to circumvent the above intrusion prevention techniques, he cannot gain access unless and until he is able to get the instruction set. Getting an instruction set in earlier versions of IPS was easy but in next generation IPS, with the use of key to encrypt the instructions and then allocating them random locations, makes it a daunting task for the attackers to guess the instruction. Furthermore, a long text encryption key is stored in a special register and when the instruction is loaded in the system, at that time each and every bit of the key is encrypted by XORing it with the corresponding encryption key. So, even if the attacker tries to execute code to extract the key, he will fail to by-pass the ISR protected key.The key can be decrypted only by using incremental approach and even if from the four byte key, the attacker tries to guess the first two bytes correctly, the random instruction will cause next two correct bytes to execute and cause the program to crash and the attacker will not be able to decipher which exact keys were guessed right as a result of randomization.

6. CONCLUSION

The next generation IPS is the result of modifications in the traditional IPS and few additional technologies such as contextual analysis and hybrid approach. It has erased all the blind spots and helped the network or system administrators to provide comprehensive security policy for their organization. With the combination of different protocols and applications, all into the next generation IPS, it tends to behave like an UTM (Unified Threat Management). UTM includes asset discovery, threat detection, vulnerability assessment, security intelligence, and behavioral monitoring. All of these aspects are included in the next generation IPS, which results in its evolvement into a Unified Threat Management system

REFERENCES

[1] Chad, Perrin. Understanding layered security and defense in depth. December 18, 2015. http://www.tech republic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/ (accessed October 20, 2015).

[2] Joel, Snyder. Do you need an IDS or IPS or both?May 2009. http://searchsecurity.tech target.com/Doyou-need-an-IDS-or-IPS-or-both (accessed October 20, 2015).

[3] Shackleford, Dave. "Real-Time Adaptive Security.". November 16, 2015. http://www.sans.org/reading-room/whitepapers /analyst/real-time-adaptive-security-34740 (accessed October21, 2015)

[4] Sophos:Ensures safe and productive web use. 2015.http://www.astaro.com/node/11367(accessed October 25, 2015).

[5] Rouse, Margaret. TechTarget: Definition of False positives in Intrusion Detection Systems. August 2014. http://whatis.techtarget. com/definition/false-positive (accessed October 21, 2015).

[6] Ganta, Victor. Winning the battle against false Positives 2006. http://www.academia.edu/1431396/False_Positives_in_Intrusion_Detection_ system (accessed October 22, 2015).

[7] Stonesoft:Winning the battle against False Positive 2006. http://pdfs.findtheneedle.co.uk/13580.pdf (accessed October 22, 2015).

[8] Hoke, Christopher. SANS:Intrusion Detection and Prevention System. November 16, 2012. https://www.sans.org/reading-room/white papers/ detection/host-base d-detection-data-loss-prevention-open-source-tools-34055 (accessed October 22, 2015).

[9] Ryutov, Tatyana. GridSec USC:Integrated Access Control and Intrusion Detection (IACID), 2015. http://gridsec.usc.edu/files/TR/TR9_IACIDRyutov. (accessed October 22, 2015).

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

[10] Hogue, Tom. Secure Data Center for Enterprise—Threat Management with NextGen. August 26, 2014. http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-secure-data-center-portfolio/threat-mgmt-ips.pdf. (accessed October 15,2015).

[11] Shinder, Deb. Windows Security:The Pros and Cons of Behavioral Based, Signature Based and Whitelist. November 13, 2008. http://www.windowsecurity.com/articles-tutorial/misc_network_security/Pros-Cons-Behavioral-Signature-Whitelist-Security.html (accessed October 24, 2015).

[12] Cisco: Applying Application Layer Protocol Inspection. 2013. http://www.cisco.com/c/en/u/td/docs/security/asa/asa72/configuration/guide/conf_gd/inspect.html#wp1383679 (accessed October 25, 2015).

[13] IPSWorks: Next Generation Intrusion Prevention System 2015. http://www.ipsworks.com /NGIPS.asp (accessed November 13, 2015).

[14] DuPaul, Neil. Application Testing Tool for performing Web Application Analysis. n.d.http://www.veracode.com/security/applicationtesting-tool(accessed November 13)

[15] Checkpoint ltd. Identity Awareness Software blade.2015.http://www.checkpoint.com/products/identity-awareness-software-blade/ (accessed November 5, 2015).