IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 4, April 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104013|

An Extensive Review of Literature on IDS and IPS

Sasikala Dhamodaran[1], Chandrakanth Dandothikar[2], Challa Sai Pranathi Reddy[3], Jitendra Teja Janapati[4]

Professor, Department of Computer Science & Engineering, JB Institute of Engineering & Technology, Moinabad, Hyderabad, India[1]

UG Students, Department of Computer Science & Engineering, JB Institute of Engineering & Technology, Moinabad, Hyderabad, India[2,3,4]

ABSTRACT:NGIPS is a cutting-edge programmed web security and hazard prevention tool examining web traffic to perceive doubtful pursuit and susceptibilities identical to phishing, web intrusions, etc. through any network. It is an all-embracing radical obstinate hazard shield that puts off the breaks, impedes invasions and defends any invaluable resources. The NGIPS is responsible for cutting-edge multi-stage AI analysis for uncovering and extenuation of future and beyond mysterious and zero-day progressive insistent coercions, APTs.

KEYWORDS:NGIPS, Powerful Intuitive Agile Automated Scalable Security Intelligence, Security, SOC, SIEM, Context Security Intelligence, Cognitive Security Intelligence, AMP, TA, TP, NDR, CVE, NGIDS.

I. INTRODUCTION

Intrusion Detection System has an IDS establishment by proactively peruse a system's inbound traffic to weed out vindictive pleas and Intrusion Prevention Systems has an IPS pattern that inhibits outbreaks by smashing malevolent packets, jamming antisocial invasion deterrence and letting know security workforces to latent menaces. Thereby IPS all the time complements IDS forever.

The Next Generation Intrusion Prevention System (NGIPS) ascertains and jams cutting-edge perils by discriminating inconsistent activities for instance sensitive data leakage, file identification, and server proscribed outreach. In doing so, making this available with all the proficiencies of ascertaining mutually the uses and the usage events on their internal setup for these organizations.

NGIPS plugs into any web deprived of foremost alterations to their hardware stipulating reliable security from corner to corner through public and private clouds for hazard avoidance and managing.

While densely cohesive security frame are contemporary, NGIPS lead into indications about latent risks and vulnerabilities with security tools beyond associated laterally with this grid setup. This is accountable for multi-level protection from dormant threats.

Characteristics of a NGIPS

NGIPS perceives and obstructs abuses. Cyber threats are attaining further hi-tech every single calendar day. For operation by such cutting-edge cyber-attacks, NGIPS typically go together with a next generation firewall (NGFW). As a lined up device, it scrutinizes and impedes traffic well-known as malevolent or unsolicited. It will moreover be installed for docile revealing, as a replacement for lined up assessment, at the perimeter, or data center dispersal. In one or the other instance, the preeminent NGIPS resolution is the one that is unwavering, consistent, and rapid for the setup it desires to defend. Additionally, it should be flexible enough to get easily integrated into existing security architecture without causing the organization to delve into a web redesign.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104013|

A steadfast NGIPS propels innately into the deep-seated security frame to consent authentic traffic to dispatch while silently obstructive for outbreaks and repelling elusion practices easily spreading refined assaults while generating as limited false positives as feasible deprived of bringing together network latency.

Furthermore, a committed NGIPS lets this institute controlling and hazard conception established on outbreak series, device-level OS data, susceptibility intelligence, user and asset views, and more.

Helps any organization to align security, compliance, and menace management with their business goals. The vital awareness is on earlier approval and optimization of the utmost fit NGIPS prototype for that organization.

With the NGIPS, more visibility, enhanced menace detection and response, are acquired as contrasted to simply enforcing firewalls on the network. Detection and jamming malware are implemented as it enters the web, or even if it just exists in at the innumerable endpoints of this network.

The NGIPS resolution eases overall costs for every business. These cohesive security resolutions upsurges and impose reliable security through their intact infrastructure. The data endowed over web visibility, security intelligence, computerization and cutting-edge risk fortification consents them to make available multi-level security from latent coercions.

Paper is organized as follows. Section II describes the Next Generation Intrusion Prevention System. The Algorithms used is discussed in Section III. Section IV depicts the Review of Literature. Section V portraysthe Applications. Finally,VI renders the Conclusion and Future Scope.

II. NEXT GENERATION INTRUSION PREVENTION SYSTEM

Next-Gen

Everything categorized next-generation (NG) infers there are many important things that require an upgrading. IDS, put up for the web as the cradle of reality, tailors that receipt.

IDS are on track from 1990s to tackle the principal risk of the time: faults in computer software. Signatures, the IDS' detection policy, have a meticulous relationship with Common Vulnerabilities and Exposures (CVE). Reasonably, signatures are the contender to the feats set up in hacking tools like Metasploit. Signatures try to ascertain the traffic configurations of famous feats in contrast to well-known software susceptibilities.

For IDS, NG can be mystifying as vendors have put the threat intelligence calling those NG-IDS. Threat intel is a vital add-on, but it doesn't discourse all the ins and outs why a next generation for IDS is necessary.

IDS has not distributed on the Full Spectrum Promise: From the start of IDS, look for configurations, delineating behavior, and finding variances were vital for full-spectrum detection (NIST 800-94). IDS creators reckoned out the configuration part, but sensing behaviors and anomalies attested indescribable as a good indulgent of standard was challenging to realize in dynamic situations by manual analysis methods. Currently, machine learning constructs the basis for NG-IDS to distribute what is profoundly deficient in out-of-date IDS: behavioral, anomaly, peer group, and rule-based configuration recognitions. This is analytically vital as it lets NG-IDS to spot well-known and mysterious attacker mysterious attacker policies, practices, and events (tactics, techniques, and procedures TTP). Then travel away from to stretch NGIDS providing multi-level shield.

Most NGIPS systems entails of signature-based detection of well-known coercions, and statistical anomaly-based detection of the anonymous also termed as behavior-based detection. These systems are predominantly suitable in the identification and mitigation of ever-evolving and zero-day advanced persistent threats (APTs).

The NGIPS provides cutting-edge multi-stage AI analysis for detection and mitigation of future and beyond unknown and zero-day APTs with the dynamic aspects provided as follows:

1. Cohesive Threat Intelligence, 2. Cutting-edge Insistent Risk Shield, 3. Precise Menace Recognition &Avoidance 4. Revision to Multifaceted Surroundings 5. Outbreak Recognition & Prevention Proficiencies 6. Intrusion Recognition & Progressive Threat Deterrence 7. Put on Intelligent Recognition and Avoidance Technology 8. Dynamic practice of Hazard Intelligence Sustains 9. Continual Monitoring by context aware customer identification 10. Endures Optimized automated blended Security Intelligence Implementations.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104013|

Attack Detection Capabilities

Intrusion Detection and Advanced Threat Prevention:

Flow-based detection: Aids IP fragment reassembly and TCP flow reassembly.

CVE-compatible signature library: Identifies and jams malware, worms, spyware, backdoor Trojans, scanning/probing, brute force cracking and other malicious traffic. Custom-coded signatures are reinforced.

Server exception discovery: Studies illicit outreach performances of a server by preset learning of the server's authentic outreach performances.

Sensitive data fortification: Spots and guards along with leakage of sensitive data (ID number, bank card number, phone number, etc.) and special files.

Botnet fortification: Implements suitable shield activities established on malevolent host and C&C server address status that is apprised in real-time.

Client-side susceptibility recognition: Enhance an application-specific susceptibility rule that includes Adobe, IE, and Office to deal with amassed outbreaks abusing client-side application susceptibilities.

Granular application management and traffic controls: Supports SCADA-based vulnerability detection and protection.

Online malware detection and blocking.

DoS/DDoS Fortification: Imparts DoS/DDoS outbreak vindications, and aids TCP/UDP/ICMP/ACK Flooding, UDP/ICMP Smurfing, and other usual DoS/DDoS outbreaks.

Deployment and Management Proficiencies

Protection Configuration aids configuration templates, and ascribes the similar fortification policies to numerous resource clusters.

Know-how to be castoff out-of-box

Extraordinary Ease of use Sustains Dynamic / Backup and Dynamic / Dynamic (asymmetric routing) distribution

Upkeeps programmed fail-over and fail-back: If a hardware or software disaster is identified, the NGIPS will inevitably switch to the circumvent channel, by no effect to traffic.

Protocol Encapsulation Sustains IPv6

Sustains IPv6 and IPv4 hybrid network deployment.

Helps encapsulation protocol such as, VLAN 802.1Q, BGP, MPLS, QinQ, PPPOE, and will get used to branched out network settings.

Management Capabilities endows Web-based remote GUI management.

Bestows centralized management.

Presents hierarchical management functions to pick up requests for tiered deployments in large-scale networks

Alert Response Procedures Upkeeps manifold alert responses, that includes, session blocking, IP segregation, email notification, and SNMP/Syslog

Advantages: •Invasion Deterrence • Hazard Intelligence • Hazard Analysis • Web Application Security • Traffic Control •Context-aware User Distinctiveness • Risk Conception •Physical and Virtual Applications. • All-inclusive and Reliable Hazard Fortification. • Scalable Fortification with Industry Prominent Price/Execution. • Easy Hazard Management.

III. ALGORITHMS USED

Powerful Comprehensive Consistent Intuitive Agile Automated Scalable Security Intelligence with Security Operation Center (SOC) and Security Incident Event Management (SIEM) blended with Context and Content based Security Intelligence providing a clear picture and extensive context for investigations, Cognitive Security Intelligence and Advanced Malware Protection (AMP). NGIPS aids time-strapped analysts with an optimized workflow that integrates detection, investigation, response and prevention into a single tool that includes the Physical Security that includes Opacity Shield Security, Cryptographic Algorithms, Machine Learning Algorithms, Deep Learning and Neural Networks Algorithms.

The Threat Analysis (TA) based broad protocol support, supports multiple file types, performs extensive static and dynamic code analysis, and virtual OS support. The Threat Prevention (TP) refers to policies and tools that protect any corporate network.

In addition to TP focused on the perimeter with an increasing array of threats such as malware and ransomware arriving via email spam and phishing attacks, currently advanced TP requires an integrated, multilayered approach to

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104013|

security including tools for intrusion threat detection and prevention, advanced malware protection, and additional endpoint security threat prevention.

NGIDS an NDR technology monitors for malicious activity and policy violations. It does it with full-spectrum detection, powered by machine learning behavioral analysis and high-risk Common Vulnerabilities and Exposures (CVE) exploit identification and a streamlined incident-response orchestration. It's also a brittle signature technology that spots threats, stops post-compromise intruders, and closes compliance gaps caused by cloud initiatives and encryption blindspots.

NGIPS can use their pre-programmed exploit-facing signatures to fire alarms to administrators, remove malicious packets, block access from offending source addresses, and reset connections.
The NGIDS and NGIPS often work together.

IV. REVIEW OF LITERATURE

SNo	Ref. No.	Concept / Algorithm Discussed	Outcome Solution	Outcome Problem	Future Scope
1.	[1]	Network intrusion detection mechanisms based on the ML and DL methods	Proposing an efficient NIDS framework using less complex DL algorithms and have an effective detection mechanism	Research variances in refining the model implementations for low-frequency outbreaks in a real-world environment and to realize efficient results to lessen complexity for the future models.	Enterprise a new, lightweight, and competent DL-based NIDS that will meritoriously spot the interlopers inside the web.
2.	[2]	8 Top Intrusion Detection and Prevention Systems (IDPS) of 2022	Actively researching cybersecurity and latest trends	Challenges When Managing IDPS: False Positives, Staffing, Genuine Risks	Approach common security encounters, also informational deep-dives on cutting-edge cybersecurity
3.	[3]	Deep superlearner for WebShell attack detection	Effectively detect WebShell, and its accuracy and recall are greatly improved	Algorithm has certain limitations in time	Improving the time efficiency of the deep tremendous learner and refining the hands-on application capability of the algorithm
4.	[4]	NB-Opcode	Improves the efficiency and accuracy of Webshell detection	Webshell sample collection is difficult, and the number of sample collections was small, resulting in over-fitting of the detection model.	These are the next issues that need to be studied and solved.
5.	[5]	Block WebShell Injections	Suggested controls and security tools	Difficult to detect because they can be hidden within seemingly innocuous files.	The tainted system endured, still when the server susceptibility was reinforced. So mitigate WebShell attacks and protect the servers
6.	[6]	Typosquatting& Cybersquatting Protection	SSL certificates	Continuously monitor all of your typosquatting threats.	Continual Monitoring & Protect from reputational damage
7.	[7]	Guard against WebShell	Patching all on-premise Microsoft Exchanged servers in the environment and continuously monitor	The go-to technique for invaders to feat susceptible Web servers for years. Established on the attainment offenders are	Sustaining fortifications high.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104013|

			networks for indicators of compromises.	partaking latterly by exhausting them, they will endure to be a prevalent method.	
8.	[8]	Protection against Exchange Server attacks	Detection by security tools	Attackers may put wrappers around it or encode it to evade detection by security tools.	Security companies tracking the activity for observing their attack patterns thereby advancing their protection.
9.	[9]	Kinds of cybersquatting and its hindrance and goals.	Prevention and targets. Enactment	Real menace to the society	Cybersquatting and other cyber menace and domain name protection
10.	[10]	Protection against Cobalt strike malware, Webshells, Data exfiltration, Misc malware, Flubot, Joker Android malware	innovative cybersecurity	Neural Networks capable of solving seemingly intractable challenges at gargantuan scale. Automated systems and attempt to solve them through the intelligent application of deep learning, at scale.	user-facing ML models and massive-scale neural networks should be a focus, expect to continue to be surprised, and to continue to adapt, as this field changes.
11.	[11]	RaaS kits	Preventing RaaS Attacks	Recovery from a ransomware attack is difficult and costly.	As an end result it's worthiest to inhibit them totally.
12.	[12]	Cloud-hosted software solutions sold by legitimate vendors to both people and businesses.	Preventing RaaS Attacks	Possible for just about anyone to become a cyber-extortionist.	Persistently scrutinizing the cutting-edge data security intimidations, and are dedicated to guarding establishments of all sizes from security breaches.
13.	[13]	Defend against RaaS	Ransomware defense strategy	Robust backup process.	For the enterprise, robust ransomware defense strategy can only fortify its cybersecurity posture.
14.	[14]	Defend against Trojan Ramnit	Ramnit uses an external script that's pulled into web sessions in real-time from its remote server.	Ramnit morphed into a banking Trojan	IBM X-Force's help
15.	[15]	Extended detection and response (XDR)	Achieve improved visibility across an organization's networks, endpoints, SIEM and more via open-system integration. XDR solution offer more automation and AI enrichments at all levels of detection, analytics, investigation and	Necessary to encounter different methods to spot and react to coercions. To crack instant and awful disputes, in mixture they've made more defy: how to practice and acquire significance from them jointly. These are point tools; they were prepared to address precise encounters. Presently that security teams	Gartner recognized XDR as the number one security and risk leaning at the completion of 2020, signifying at present moment when all this difficulty — too many tools, too many alerts, too little time — is imminent ahead, with XDR as a reply.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104013|

			response.	façade a limitless encounters, it's constantly existed more acute to have them operate in concert. Underprivileged of undertaking it, narrow security task assets will endure to be put out weak, full cost of proprietorship will endure to upsurge and the procedure of pinpointing and retorting to intimidations will stay to be time-consuming and ineffective.	
16.	[16]	LockBit 2.0	Activity and an analysis of the new payloads of LockBit	X-Force researchers were able to identify files submitted to VirusTotal in August 2021 that may be samples of the StealBit malware, but analysis is still ongoing at the time	novel technique for deployment LockBit is a Growing Threat to Watch For
17.	[17]	Best Practices to Counter Common Cybersecurity Risks	New and bigger solutions. Review common best practices like password policies, least privilege access, patching and more to assess and control today's risks.	Choosing the right tools for the job.	As invaders realize innovative techniques to feat loopholes and susceptibilities, the good guys must adjust with these methods to be one stage ahead.
18.	[18]	Defensive perspective for Webshells	Detect web shells and protect the assets	Web shells might also not get detected by antivirus or anti-malware software because they do not use typical executable file types.	Numerous web servers are set up in such a way that even a meek script is adequate to cause major harm. This is the core aim as to why there are thousands of overtly available web shells. The fact that so many variations exist makes it difficult for intrusion detection & intrusion prevention systems (IDS/IPS) to detect them, especially if they are using signatures to detect such web shells. Specific web shells are very refined and they are almost dreadful to spot, even with behavioral analysis.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104013|

19.	[19]	Optimized support vector machine (SVM)	The total accuracy (combining all the web shells & benign scripts) is 92.18%, & 95.26% of web shells can be detected successfully	The aspects applied in this paper are generally statistical-centered.	1. Coverage of this method needs to be improved. Future work is to study the mechanism of web shells with other languages, such as JSP, ASP, & Python. Goal is to find a general way to detect different types of web shells, e.g., using a system log to detect web shells in real-time. 2. Feature engineering can be improved. The aspects applied in this paper are generally statistical-centered. Future work is to use deep neural networks to extract & select features automatically, e.g., using auto-encoding & decoding
20	[20]	Netsparker	High-quality dynamic application security testing (DAST) solution	Usually involve many stages & may be prepared & executed over a long period of time.	As web shells are so hard to find once installed, prevention is especially important. To minimize risk, follow the best practices for web server & application hardening

.

V. APPLICATIONS

NGIPS proctors web traffic to spot distrustful commotion and susceptibilities like phishing, web intrusions, etc. through this network. Most NGIPS schemes comprises of signature-based detection of notorious intimidations, and statistical anomaly-based detection of the mysterious.

The NGIPS is responsible for all-inclusive hazard defend that impedes invasions, averts breaks, and upholds this invaluable resources.

NGIPS a progressive programmed web security and hazard hindrance tool plugging into any network without most important alterations to its hardware.

NGIPS verves outside signature and behavior-based detection, with cutting edge Intelligent Detection, innovative intelligence heuristics learning technology for web and application hazard detection totaling optional virtual sandboxing competency. Threat Analysis System (TAS) customs manifold innovative detection engines to ascertain well-known and zero-day APTs, together with IP reputation engines, anti-virus engines, static and dynamic analysis engines and virtual sandbox execution simulating live hardware statuses. Finally coalescing AI with present-day threat intelligence to become aware of malevolent sites and botnets thus leveraging the power of Powerful Wide-ranging Steady Innate Agile Programmed Scalable Security Intelligence with NDR technology, SOC and SIEM blended with Context and Subject based Security Intelligence, Cognitive Security Intelligence and AMP to furnish all-encompassing security, more control and faster performance with the NGIDS and NGIPS habitually work systematized for the best security process.

VI. CONCLUSION AND FUTURE SCOPE

NGIPS resolution mixes IPS with application control and influences the power of Powerful Comprehensive Consistent Intuitive Agile Automated Scalable Security Intelligence with NDR technology, SOC and SIEM blended with Context and Content based Security Intelligence, Cognitive Security Intelligence and AMP. Autonomous AI to

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104013|

dispense all-encompassing security, more control and faster performance with the NGIDS and NGIPS every so often work in collaboration for the preeminent security process. IDPS is an enduring process with enhanced security, more control and quicker enactment as an augmenting persistent NGIDS and NGIPS executions abstaining for the future ahead.

REFERENCES

[1] Zeeshan Ahmad, Adnan Shahid Khan, CheahWaiShiang, and Johari Abdullah, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches", Transactions on Emerging Telecommunications Technologies, John Wiley & Sons Ltd, vol. 32, no. 1, pp. 1-29, January 2021.
[2] 2. Kyle Guercio, "Best Intrusion Detection and Prevention Systems for 2022: Guide to IDPS", eSecurity Planet, December 22, 2021.
[3] Zhuang Ai, NurbolLuktarhan, AiJun Zhou and Dan Lv "WebShell Attack Detection Based on a Deep Super Learner", Symmetry , vol. 12, no. 9, pp. 1-16, 2020.
[4] You Guo, Hector Marco-Gisbert, and Paul Keir, "Mitigating Webshell Attacks through Machine Learning Techniques", Future Internet, vol. 12, no.1, pp. 1-16, 2020.
[5] Edward Kost, "What are Web Shell Attacks? How to Protect Your Web Servers?",UpGuard, Cybersecurity, January 11 2022.
[6] AbiTyas Tunggal, "What is Typosquatting (and How to Prevent It)", UpGuard, Attack Surface Management, August 22, 2021.
[7] Joan Goodchild, "What You Need to Know -- or Remember -- About Web Shells", Dark Reading & The EDGE, Cybersecurity In-Depth, March 30, 2021.
[8] Kelly Sheridan, "Inside the Web Shell Used in the Microsoft Exchange Server Attacks", Dark Reading &The EDGE, Attacks/Breaches, March 23, 2021.
[9] SapnaSukrutDeo and SukrutDeo, "Cybersquatting: Threat to Domain Name", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 654, pp. 1432-1434, April 2019.
[10] Sophos 2022 Threat Report, "Interrelated threats target an interdependent world", SOPHOS Cybersecurity evolved, 2022.
[11] CROWDSTRIKE, "RANSOMWARE AS A SERVICE (RAAS) EXPLAINED", BLOG, January 28, 2021.
[12] Michael Peters, "What Is Ransomware-as-a-Service? Understanding RaaS", Ransomware-as-a-service lowers the bar for entering the entering the cyber extortion game, Security Boulevard, February 6, 2019.
[13] Mark Stone, "Everything You Need To Know About Ransomware Attacks and Gangs In 2022", SecurityIntelligence, January 3, 2022.
[14] LimorKessem and ItzikChimino, "Top-Ranking Banking Trojan Ramnit Out to Steal Payment Card Data", SecurityIntelligence, January 31, 2022.
[15] ThibaultBarillon, "What Is Extended Detection and Response (XDR)?",SecurityIntelligence, October 12, 2021.
[16] Megan Roddie, "LockBit 2.0: Ransomware Attacks Surge After Successful Affiliate Recruitment", SecurityIntelligence, September 9, 2021.
[17] AbhishekSengar, "Try These Best Practices to Counter Common Cybersecurity Risks", SecurityIntelligence, May 25, 2021.
[18] AgathoklisProdromou, "An Introduction to Web Shells Part 1", "Web Shells 101 Using PHP Part 2", "Keeping Web Shells Under Cover Part 3", "Web Shells in Action Part 4", "Detection & Prevention Part 5", The Acunetix BLOGs, Web Security Zone, April 16, 2020.
[19] Tiantian Zhu, ZhengqiuWeng, Lei Fu and LinqiRuan, "A Web Shell Detection Method Based on Multiview Feature Fusion", Applied Sciences, vol. 10, no. 18, pp. 6274-6290, September 2020.
[20] ZbigniewBanach, "How Web Shells Work", Netsparker, Web Security Blog, 16 October 2020.
[21] GilangIntanPermatasariDuppa, and NicoSurantha, "Evaluation of network security based on next generation intrusion prevention system", TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 17, no. 1, pp.39-48, February 2019.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details