Survey: Current Web Application Security trends in Cyber Security Attacks and the Difficulties of Implementing a NGFW to Defend Against Them

Danel Batyrbek
School of Engineering and
Digital Sciences
Nazarbayev University
Nur-Sultan, Kazakhstan
Email: danel.batyrbek@nu.edu.kz

***Abstract*—In the current day, when new discoveries and advancements are being made in almost every field of Computer Science, the inherent cyber security risks seem to follow those advancements. Much effort is being spent to devise new technologies and best practices to diminish the risk of cyber security threats and decrease the number of successful cyber attacks. Despite the best efforts, however, the number of successful cyber attacks and data breaches doesn't seem diminish, but instead grows bigger every year. When after every attack or a data breach businesses and institutions suffer big expenses and monetary losses, one question that comes to mind: why does this keep happening, despite the best efforts to prevent it? This survey paper intends to explore the cyber security trends and advancements in Next Generation Firewall (NGFW) technology and see where it is falling short to prevent security incidents. One of the observations is the difficulty of setting up NGFW correctly. The survey paper will try to propose how the new successful model of a NGFW should look like to address the impeding threats in the future.**

I. Introduction

Internet has opened a world of new possibilities. Internet allows you to integrate with many services and institutions which allow you to do online shopping, get health services and even loan money. The Internet has brought together many people and tools, which in turn given a rise to many advancements and discoveries. Despite all the benefits of the Internet, however, there are major consequences which range from disturbing to life-threatening. The Internet wasn't conceived with a security in mind. Security researchers put a lot of energy into improving the security of the Internet. This brought forth many vulnerability scanners and firewalls.

Firewall is a tool that operates on the network level and filters the packets depending ports, ip-addresses and on the configured rules. The main vector of attack, however, that remained uninspected is a Hyper-Text Transfer Protocol (HTTP). The need for an enhanced security brought forth the concept of the Next-Generation Firewall (NGFW). NGFW was developed to have the features are the security experts believed was necessary to defend against adversaries. One of the reasons that the hackers are able to get a foothold in the network is the lack of monitoring of network activities. Thus appeared the network monitoring. Many of the vulnerabilities are in the Web Application or the Web Server itself. The inspection of the contents of the requests was needed. The Deep Packet Inspection (DPI) was introduced. The problem with DPI is that it can operate only on the known attack signatures, and thus doesn't protect from the unknown attack vectors. Detection of abnormal behaviour in the network activity or requests is required. Thus the anomaly detection was developed.

Much work was done by many leading researchers and engineers in this fields. So much, one would expect that the number of successful cyber attacks would become extremely low. As some researchers have analyzed, the number of successful cyber attacks has diminished. [1]. But the number is not as low, as expected.

The question is "Why the new NGFW technology fails at preventing the further spread of cyber attacks?". This survey paper will analyze the characteristics of the cyber attacks, the current capabilities of the NGFW and will try to propose the features that the NGFW needs to have to face the current and maybe future challenges in cyber security world.

II. Literature Review

The researchers have made a literature review concerning the cyber security trends and firewalls. When researching the attack trends, the papers of Daljit and Devanshu provide an overview of the trends in the recent years. [1][2] The presence of black market on the dark web also contributes to the current cyber security trends. Survey paper from Huang and other researchers explores the dynamics of buying hacking services on dark web and compares the cost with the possible profit from the successful attack. [3]

Literature regarding the firewalls was reviewed as well. Kishan, Rami and Lei give an overview of NGFW, what problems the NGFW attempts to solve and how. [4] There are also comprehensive papers on anomaly and intrusion detection techniques. [5][6] Additionally to that, the papers that explore the different problems of NGFW, like 3rd party vendor integrations [7] and expressiveness of the configuration interfaces of the firewalls [8] were reviewed. Some papers attempt to provide the solution to the current model of NGFW,

in an attempt to solve the problem of increasing workload [9] and the effectiveness of enforcing the security policies in the network. [10] But the research showed that there are problems with the NGFW that can circumvent the security configurations: namely SNI bypass [11] and firewall rules fingerprinting. [12]

III. Cyber Security Trends

As it currently is, there are two main team specializations that constitute the Cyber Security field: Attack Team and the Defense Team. Attack Team describes hackers that perform penetration tests: real-life-like simulations of hackers' attacks in an attempt to find vulnerabilities and as a result, compromise the target system. The Defense Team is a team of specialists that focus all of their knowledge of Cyber Security trends to prevent the successful cyber attacks and minimize the risks.

There is an ongoing research in both of the fields. The developments in Attack Team constitute different exploits, tools and frameworks that assist in the penetration tests. The Defense Team's developments, on the other hand, are different tools and frameworks that assist in filtering of malicious payloads, analysis and patching of vulnerabilities.

As many more advancements are being made in both of the teams, the new fields and directions emerge. For example forensic investigators are required to have a practical knowledge of exploitation methods, but also an understanding of the defense practices and mechanisms. The code review on the other hand is seemingly far from both of the teams' main activities, but is an cornerstone of the effective security. Many new emerging fields arise from the mix of the Attack and Defense Teams' methods with other fields in Computer Science or outside of Informational Technologies.

Although there are many types of cyber threats and exploitation methods, the primary focus of this survey paper is the Web Application attacks, since the Internet is starting to have a more prevalence in our life, and so do the Web Application attacks.

IV. Attack Team

The primary source of security vulnerabilities are program bugs and (or) design flaws. The vulnerabilities differ from each other in terms of bug cause, exploitation ways and impact. After systematically reviewing different vulnerabilities and categorizing them, the list of top dangerous vulnerabilities was compiled. It is called OWASP TOP-10.

OWASP TOP-10 is a list of top 10 vulnerabilities found throughout the year, ranked based on their impact and difficulty of exploitation. It is compiled by Open Web Application Security Project (OWASP) and updated each year.[13] What researchers have found, however, is that the rankings hardly ever change. [1] The most ranked vulnerabilities stay the most ranked. Namely, despite the awareness about the danger of SQL injections, they are still one of the most exploited vulnerabilities to this year. [1]

Down is the list of vulnerabilities from OWASP TOP-10 2020, as they appear on the list:

Injections

Injections is a class of vulnerabilities, where the hacker has an opportunity to inject a piece of code or command and compromise the stability of the system and/or take a control of the said system. [13]

Broken Authentication

Broken Authentication refers to a class of vulnerabilities, that allow to bypass or circumvent the improperly implemented authentication mechanism. The hackers do so by gaining information about usernames, passwords, tokens, etc. from the authorization mechanism and as a consequence assume the identity of the other user on the system.

There are different ways to circumvent the authentication mechanism. Some might employ SQL injections, others might use the language's in-built features, like PHP's loose type comparison (a.k.a. type juggling). [13]

Sensitive Data Exposure

Sensitive data exposure refers to vulnerabilities, that allow the hacker gain an unauthorized access to the confidential information via the exposed APIs and the lack of identity checks and access controls.

XML External Entities (XXE)

XXE is a class of vulnerabilities that occurs when the hacker has an opportunity to craft an XML object and pass it to an XML parser. When the parser implicitly trusts the user input, it can execute commands on behalf of the hacker.

Due to the verbosity and capabilities of the XML standard, the XXE pose a serious threat. The possible effects of the XXE are: remote code execution, local file inclusion, server-side request forgery, internal network enumeration and even denial of service. [13]

Broken Access Controls

Access controls are one of the fundamentals that constitute security. When the access controls are broken and the users are given the opportunity to see/edit/delete data they are not supposed to be able to, then it compromises the security and the trust of the system. If the users, on the contrary, are not able to perform the actions they need to perform, then it can result in a denial of service. [13]

Security misconfiguration

Security misconfiguration is one of the most perverse bugs, as it is difficult to track them down and properly evaluate risks of the misconfiguration. Security misconfigurations often can give access to a restricted parts, expose sensitive data, like the server configuration and thus, put the security of the system at risk. [13]

Cross-Site Scripting (XSS)

XSS occurs when an untrusted JavaScript reaches a victim's browser and executes malicious payload. Hacker can either attempt to store the malicious JavaScript code on the target site (Stored XSS), or give the victim a specially crafted link, which triggers a XSS vulnerability, when clicked on it (Reflected XSS). It is also possible to create a malicious browser extension which changes the DOM-view of the page and injects the malicious JavaScript (DOM-based XSS).

Due to the nature of the JavaScript, the hacker is able to do everything the JavaScript can. The XSS attacks are used in Social Engineering attacks, to hijack user session or even Remote Code Execution, if coupled with the browser sandbox escape techniques. [13]

Insecure Deserialization

Deserialization is the process of taking a textual description of some object and loading it into the memory. While many modern languages provide a deserialization, it is also possible to deserialize class objects and their methods. The insecure deserialization can lead to remote code execution, privilege escalation and many other detrimental consequences. [13]

Using Components with Known Vulnerabilities

When the vulnerability is discovered, the accompanying exploits and tools become available in the matter of days or weeks. This creates an opportunity to exploit the systems that are dependent on those components. [13]

Insufficient Logging and Monitoring

Creating a complex system without security vulnerabilities requires an insurmountable amount of effort. Something, which is not currently possible with the current requirements that the business imposes on Software Engineering. Thus, there are bound to be vulnerabilities, one way or another. To prevent the further escalation of the hacker and to confirm the state of security, the logs need to be constantly monitored.

Insufficient logs may not provide the necessary information that would show the signs of compromise. Even if such logs exists, not reviewing the logs is the same as not having the said logs. [13]

V. Web Attack trends

Based on the empirical analysis of web application attacks by Daljit Kaur and Dr. Parminder Kaur, we can say that the number of the cyber security attacks has diminished. Despite that, the most exploited vulnerability was and still is an SQL injection. [1] This is also confirmed by Devanshu Bratt and OWASP TOP-10.

The analysis showed that the sites in Government, Educational, Social Networking, and game downloading categories are most often the target of cyber attacks. [1]

Government websites also lead in almost every vulnerability counts based on the type. The only exception are the DNS Hijacking and Unauthorized access. This can be explained by the tight security policies that are employed by the security experts at the governmental institutions. Educational websites have the most defacement attacks.

More and more attacks are being executed by the help of botnets, as such, based on the Devanshu Bhatt's research, out of 93% of the reported financially motivated cyber attacks, 77% of them were exploited by botnets and 32% exploited SQL injection attacks. [2]

Although, the diminishing number of cyber attacks may be a good indicator at first, it still doesn't prove that the danger of cyber attacks have diminished. On the contrary, with the progress that is being made on detection of cyber threats, the attacks that successfully reach the target are more dangerous than they were before.

One of the reason the cyber attacks have become more dangerous, is the result of the progress that have been made in an attempt to make software more secure. In an attempt to bypass the new firewall attack detection rule or an Address-Sanitizer, the hackers become more creative with their attacks. The attacks that do bypass the security measures, inherently have a high-level of complexity. Another approach is to find other aspects of security that haven't been exploited yet. It may be a seemingly trusted SQL query, susceptible to router SQL injection attack, or an organization employee, who is not aware of possible consequences of a Social Engineering.

Another explanation is that the cybercrimes have become more organized. Namely, there are services on the dark web that allow to buy different cyber attacks for bitcoin. [3] Such business provide different services and allow to combine them with each other. The price is relatively affordable, and if the attack is successful, then the value earned from the successful hack outweights the cost of the attack. One such example is by chaining exploit with a payload, obfuscating or repackaging it and automating with a botnet. The said elements can be provided by Exploit-as-a-Service (EaaS), Payload-as-a-Service (PLaaS), Obfuscation-as-a-Service (OBaaS), Repackage-as-a-Service (RpaaS) and a Botnet-as-a-Service (BNaaS), which constitute only a small number of the existing cybercrime services. [3]

Such measures are employed for different reasons, ranging from compromising business activities with a ransomware, to using botnets to generate a fake or a malicious reputation. It is even possible to largely scale the attacks against different segments other than the Web, like mobile infrastructure, hardware, firmware and IoT. [3]

VI. Next Generation Firewalls

As it was clear from the previous section, the are different types of vulnerabilities. The combination of different vulnerabilities opens up a space of many possibilities, and as such, many detrimental consequences. Only assessing the security of the systems is not enough. It is not possible to ensure that all vulnerabilities have been identified with a penetration test and sometimes fully mitigating the vulnerability is not possible. Thus, it is important to develop tools that can provide an additional layer of security, other than the in-built security mechanisms.

One such solution is a firewall. Firewall is a network-layer application that is capable of filtering the packets, depending on the given characteristics and filtering rules.

The first firewalls were very primitive. [4] All they could do, was filter the packets based on the port number and IP addresses, both source and destination. This was rather simple to implement. However, it is soon proved to be ineffective, since many of the vulnerabilities were exploited via HTTP protocol. Blocking the access to the HTTP is impossible, as it would contradict the goal of having the website in the Internet in the first place.

Because of that, the new model of Firewalls was required. It was called a Next-Generation Firewall (NGFW). The new class of firewalls had the same capabilities of the previous generation, as well as the new features that help to focus on more prevalent problems of the web application security. [4]

NGFW FEATURES

A. Deep-Packet Inspection

Important features that set apart previous firewalls from NGFW, is a Deep Packet Inspection (DPI). DPI inspects the incoming packets for a possible malicious payload and takes action upon finding such packet. This gives an opportunity to inspect the HTTP and Application layer. NGFW can also decrypt and inspect encrypted packets.

B. DDoS Prevention Mechanisms

Some NGFW can detect the distributed Denial of Service (DDoS) attack attempts. By blocking the source address or the user session temporarily, it can prevent many stability problems of the Web Application.

C. Application Awareness

By making NGFW aware of the application traffic, it becomes possible to catch and block suspicious packets. Many malware try to hijack authorized processes, to evade the antivirus. When an authorized application starts to send unusual or suspicious packets, then it is a sign of compromise.

D. Anomaly Detection

Another important feature that the NGFW implement is the anomaly detection. New attack methods are being devised every day and it means that it is not possible to always keep a signature database with all of the possible attacks. One of the measures against the possible undiscovered attacks is Anomaly Detection.

Anomaly detection can be applied to many instances. For example if you have a website with many visitors every day, then it is possible to collect data about the ”standard” user behavior. As such, when the users start to access the web pages to which the users usually don't have an access, or start to submit an input that is very different from the usual expected input, this constitutes an anomaly and may hint to an ongoing incident. Another application of anomaly detection is when the network traffic inside the corporate network is being sampled and the abnormal packets may suggest that the intruder is inside the network.

E. Identity Management and Access Controls

Identity management is a crucial aspect of the security, since it is important that only an authorized person has an access to a confidential information. This gives the firewalls an opportunity to enforce the stronger access control measures, e.g. giving access to a server only to an authorized person. This also allows for more enriched logs, which contain the identity of the actor, thus giving more information for incident response and investigations.

PROBLEMS OF NGFW

Although, as good as it sounds, there are many problems with the current NGFW.

A. Performance vs Accuracy

The first problem of NGFW is that they are implemented with an inherent tradeoff between the performance and the quality of inspection. As the firewall operates on the network layer, it is important that all of the devices on the network layer are fast, to avoid congestion and packet loss. Packet inspection, on the other hand, is very costly operation, in terms of performance and resources. Because of that, NGFW developers strive for a faster operations and build-in the necessary operations inside the chipboard of the firewall. [14] That being said, it is still possible to overwhelm the firewall with packets. For that reason, the developers ship NGFW with an option to choose the level of inspection, from **LOW**, to **MODERATE** and **FULL**. Because of that, using DPI comes down to managing risks.

B. 3rd Party Vendor Integration

The NGFW also have troubles integrating with the 3rd party vendors. Those 3rd party vendors may provide threat intelligence, additional extensions of NGFW capabilities or other needs that are not covered by NGFW. This imposes challenges, as the additional features require computational resources, which in turn affect the stability of the NGFW. The API to the 3rd party vendors may have challenges with integration as well. [7] As such, it is not known if the NGFW development is held to the same standards as the secure software development.

C. NGFW Mechanisms Bypass

Another problem of the NGFW, is that even with all of the measures in place, like DPI and Anomaly Detection, it is still possible to bypass the firewall and successfully execute the attack. NGFW are not full-proof.

D. Difficulty of setting up

NGFW sometimes are difficult to setup. Having many features means that there is a high-level of complexity of the firewall. With many vendors trying to sell the same product to different clients, propositioning their solution as ”one-size-fits-all”, means that they need to provide a large level of customisability of the rules and features. This results in a difficulty of not understanding what options stand for and prevents from

implementing the configurations that the users have in mind, which in turn can lead to security misconfigurations.

E. Expressiveness

As the Lorenzo Ceragioli with his other researchers have discovered, not every firewall is equally expressive. What it means, is that the rule syntax may not allow to specify the configurations that an expert intended. This can lead to risks, such as the misconfiguration or the possible workarounds that can cause vulnerabilities. [8] Not every developer of firewall engine assesses the expressive power of the syntax, since it is a formal and very mentally difficult task. Some firewalls may use older firewall management tools, like `iptables`, which seemingly give them the expressive power. Yet, when adding another interface on top of `iptables`, the interface may limit the expressive power of the `iptables`.

F. Single point of failure

Since the NGFW is an only solution (currently) that has the ability to examine application traffic, makes sense to put NGFW instance to examine all of the traffic. Yet, the NGFW are costly, thus the organizations are limited to one NGFW instance.

The NGFW may be placed between an Internet and a DMZ, which makes the internal traffic implicitly trusted. This leaves the internal traffic uninspected. Or the NGFW may be a centralized point, which inspects all of the network traffic, including the internal. In both cases, assuming that there is only one instance of NGFW, the failure of NGFW to operate would inhibit the traffic flow, leading to downtime and connectivity issues.

G. Rules fingerprinting

It is an experimental approach, but it is possible to "fingerprint" or deduce the rules that are employed by the firewall. As Isabell Schmitt and Sebastian Schinzel have shown that the process can be automated and different rules characteristics can be assessed, such as the denied/allowed methods, filtered requests and even rate-limit. [12] Unfortunately, there is no real solution against such attack, other than the blocking the hacker from the network. This is detrimental, as when using NAT, the firewall may block the normal users who happen to share the same network with the hacker. This in turn can lead to a bad reputation risk.

H. Inherently insecure protocols

The NGFW are designed to solve a very difficult task: to add additional security to inherently insecure protocols. The Internet Task Force is working on overcoming the shortcomings of the initial versions of the protocols, in regards to speed and security. But some aspects of the protocols make it an impossible task to achieve the wanted results. One such example is the Server Name Indication (SNI) bypass. Researchers were able to write and test a browser extension that allows to bypass different firewall restrictions based on SNI, due to the design flaw with the SNI itself. [11]

I. Social Engineering Vector

This is may not be directly a problem of the NGFW itself, but it is a consequence of a strong technological solutions that are employed by the NGFW. Although the NGFW may protect from the known attacks, it is still a challenge to protect the web application against the misuse. The NGFW also doesn't prevent Social Engineering attacks, like phishing. Richard Caralli and William Wilson argue that the cyber security is not just a technological aspect of the company, but an organizational problem. [15] The untrained staff with an access to sensitive information can compromise the company if they fall a victim to a phishing attack.

J. Price

Another problem is that the NGFW are highly costly. Because the cost of having a NGFW and also paying for a support of the said NGFW are not always manageable by some companies, they consider the option of having their infrastructure in the "cloud". With this option, the organization only needs to worry about the resources that are allocated to it, while the management of the cloud's firewall is the cloud provider's responsibility. Occasionally this option proves to be more cost-efficient.

K. Migrating to cloud

Regarding the Cloud-as-a-Service option, it may look like a good solution, but it doesn't solve the underlying problem with the firewalls, but shifts the responsibility to a cloud service provider. Being in the cloud means being distributed. Different clients may have different needs regarding the firewalls. Thus the rules must be dynamic. [9] Other than that, the listed problems still apply to the firewalls for the cloud providers.

VII. Discussion

Firewalls are an important defense mechanism that is employed and should be employed by every small and large organization that wants to protect its assets. Yet, it is clear that the current NGFW have limitations, in terms of technological and designed capabilities aspects.

One of the largest problems that needs to be addressed is the capability to bypass the DPI. DPI can determine if the packet contains an attack or not, depending on many known attack signatures. But because of that, the hackers are implementing different obfuscation and repackaging techniques, which increases the scope of possible malicious inputs to a new level. The NGFW is yet to learn to effectively analyze the obfuscated input.

Another problem that is a consequence of a DPI is the performance. DPI is a costly operation. One of the network requirements is speed and reliability. Having NGFW in-between the internet and the web application can significantly affect the roundtrip time. The delay can be further increased by the increasing the number of packets coming to NGFW.

Another problem that the users of NGFW face, is the need for efficient configuration. Since many NGFWs are proposed as a solution that is applicable to any organization, it usually

comes down to the fact that the NGFW doesn't fully solve all of the problems it intended to solve or behaves differently, than was initially expected. What is important for NGFW to have, is a high-level of customization, being able to adopt the NGFW to the specific needs of the organization, and do it efficiently. What NGFWs also need, is the tool or some mechanism to assess the correctness of the configuration. This is a difficult task, which may not be achievable currently, due to time-wise, economical and technological constraints.

As a result, the new NGFW model needs an efficient mechanism for packet analysis and a distributed model that can handle large amount packets. The model also needs to be high level of customization and a verification tools of such configuration. The NGFW is also needs to be relatively cheap, to allow small and large companies and organizations setup their own NGFW.

Possible Solutions

The efficiency of the DPI

One of the solutions to increasing the DPI is to use a "Misuse detection". This approach has its benefits, as the correctness of the packets is analyzed. The misuse detection needs to be adapted to the underlying application that is being protected. Either specify the "correct" behaviour with configurations or train the AI to detect the "correct" use from the "misuse". The efficiency of this method needs to be assessed.

Increased load

To solve the problem of an increased load on a firewalls, it may be needed to implement a distributed firewall model. The idea is to use the devices on the network as a part of the firewall, using specialized software. This is good in theory, as the new firewall model doesn't exclude the older generations firewalls and uses them as a fallback option. [10] The problem with this approach, however, is that there are still speed considerations that need to be taken into account. Another problem, is that the NGFW models usually employ a specialized hardware, due to performance. Making a distributed NGFW model with small specialized pieces of hardware is questionable. But the benefits of this approach are still to be explored.

Efficient anomaly detection

Rhongho Jang with their team propose a new model for efficient anomaly detection. One of the ideas is to use a DRAM and the other is to use algorithms that slow down the packet flow and handle the memory size restrictions. The new algorithm has tradeoffs, but if the anomaly detection can be used to analyze the subset of the packets, then this may prove useful in enhancing the security. [6]

The topic of IDS and anomaly detection is a new and emerging domain. It has a theoretical foundation and it can be applied to the NGFW. However, the methods can be mostly divided into two groups: those that search for known signatures, those that search for deviations from the standard protocols and hybrid. [5] [16] The efficiency of those detection methods needs to be assessed under real-life conditions.

Ethical considerations

For this survey paper, the ethical aspects of this research have been studied. And as such, there are some concerns have been established:

1) Privacy
2) Censorship
3) Misuse

The development of firewalls have showed that many solutions lack the visibility into the traffic activity, needed to make judgements on filtering actions of the said packets. As such, binding the traffic to a specific user and decrypting the traffic can lead to good results in case of cyber incident. But the problem with this approach is that it may inhibit the privacy of the users, for the sake of security.

Another problem is censorship. Although, the NGFW's purpose is to protect the ingress devices, it can be used limit the access to a known malicious websites. The problem arises when the owners or maintainers of the NGFW would start to use it capabilities to limit access or censor some valuable information.

The inherent problem with all of the tools, is that they may be misused. This is a problem that is a direct consequence of many security tools used for assessment and penetration. The use of such tools is justified, if the result of using such tools is a better security. Similarly, their use is considered malicious, when the use of such tools is a direct consequence of the malicious intent of the actors. The same argument can be stated about the NGFW, when the NGFW are used to protect the infrastructure that is used to make a positive impact, compared to infrastructures that bring harm.

VIII. Conclusion

There is a considerable effort being done in an attempt to create and improve the NGFW model to best serve the needs of the current cyber security age. But with the new advancing cyber threats, the NGFW need to be able to face the challenge.

There firewalls have advanced many-fold throughout the years. But the practice has shown that he firewalls can't help to defend against the misuse of the web application. The best attempt at making the web application secure is by following the Secure SDLC practices. But it is a difficult and costly process, which needs to be supervised by an expert and may not be flexible enough to adopt the constantly changing business requirements. [1]

In conclusion, it is clear that much more of the research is being done on identifying and developing new attack vectors rather than on the firewalls. There are still many problems with the firewalls that require the research and need to be tested in the real use-case environments.

References

[1] D. Kaur and P. Kaur, "Empirical analysis of web attacks," *Procedia Computer Science*, vol. 78, pp. 298–306, 2016.

[2] D. Bhatt, "Cyber security risks for modern web applications: Case study paper for developers and security testers," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 7, pp. 232–235, 2018.

[3] K. Huang, M. Siegel, and S. Madnick, "Systematically understanding the cyber attack business: A survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, pp. 1–36, 2018.
[4] K. Neupane, R. Haddad, and L. Chen, "Next generation firewall for network security: A survey," 2018.
[5] D. Singh and R. Kulhare, "Survey paper on intrusion detection techniques," *INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY*, vol. October 2007, pp. 329–335, 2007.
[6] R. Jang, S. Moon, Y. Noh, A. Mohaisen, and D. Nyang, "A cost-effective anomaly detection system using in-dram working set of active flows table: poster," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 286–287.
[7] "White paper: The threat intelligence challenges with next-generation firewalls," Bandura Cyber, Inc, Tech. Rep., 2020.
[8] L. Ceragioli, P. Degano, and L. Galletta, "Are all firewall systems equally powerful?" in *Proceedings of the 14th ACM SIGSAC Workshop on Programming Languages and Analysis for Security*, 2019, pp. 1–17.
[9] Y. Bangur and V. Mandraha, "Enhancing firewall for serving the distributed security requirements for cloud," *International Journal of Computer Science and Information Technologies*, vol. 6, pp. 2461–2466, 2015.
[10] S. Ioannidis, A. D. Keromytis, S. M. Bellovin, and J. M. Smith, "Implementing a distributed firewall," in *Proceedings of the 7th ACM conference on Computer and communications security*, 2000, pp. 190–199.
[11] W. M. Shbair, T. Cholez, A. Goichot, and I. Chrisment, "Efficiently bypassing sni-based https filtering," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, 2015, pp. 990–995.
[12] I. Schmitt and S. Schinzel, "Waffle: Fingerprinting filter rules of web application firewalls." in *WOOT*, 2012, pp. 34–40.
[13] "Owasp top ten," 2021. [Online]. Available: https://owasp.org/www-project-top-ten/
[14] "White paper: Understanding the next generation firewall and its architecture," Allied Telesis, Tech. Rep., 2016.
[15] R. Caralli and W. Wilson, "The challenges of security management," 01 2004.
[16] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, "Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 52, no. 2, pp. 1–40, 2019.