

## NIST Cyber Security Framework Development for Website Information Collection

Firdan Rafi Nugroho<sup>1</sup>, Fiby Nur Afiana<sup>2</sup>, Adam Prayogo Kuncoro<sup>3</sup>

<sup>1,2</sup>Technology Information Department, Universitas Amikom Purwokerto, Banyumas, Indonesia, 53127

<sup>3</sup>Informatic Department, Universitas Amikom Purwokerto, Banyumas, Indonesia, 53127

e-mail: <sup>1</sup>Firdanrafi241@gmail.com, <sup>2</sup>fiby@amikompurwokerto.ac.id

<sup>3</sup>adam@amikompurwokerto.ac.id

Submitted Date: July 01<sup>st</sup>, 2024

Reviewed Date: July 19<sup>th</sup>, 2024

Revised Date: July 24<sup>th</sup>, 2024

Accepted Date: July 27<sup>th</sup>, 2024

### Abstract

The rapid development of websites has made them one of the most important modern information media. However, this growth has also highlighted the critical need for robust website security to protect the data and information they contain. The website *dobelhost.com* was analyzed for security vulnerabilities, revealing several issues, including the absence of the X-Frame-Options header, the lack of an HTTP Strict Transport Security (HSTS) policy, the disclosure of server information through the X-Powered-By header, the absence of a Content Security Policy (CSP) to guard against XSS attacks, and the presence of mixed content. To address these vulnerabilities, the study employed a comprehensive method involving information gathering, implementing security headers, updating software and plugins, and enforcing HTTPS. The results demonstrated significant improvement, effectively resolving the identified vulnerabilities. This research provides a useful reference for the development or enhancement of similar websites, increasing awareness and vigilance against potential threats, and achieving better cyber resilience. The research has been completed successfully, demonstrating the effectiveness of the proposed method in resolving the identified security issues.

Keywords: Security; website; NIST; software; Hacking Threats

### 1 Introduction

Cyberspace is a computer system consisting of various services, systems, installed processors, controllers, and information stored or transmitted over the network. The development of internet technology brings various conveniences, experiences, and entertainment to its users, such as ease of access, processing, and easier global use (Sulistiyowati et al., 2023). However, the increasing threat of cyberattacks every year cannot be separated from the vast benefits offered by the internet. The increase in the number of cyberattacks is fueled by the ever-increasing popularity of the internet (Garba et al., 2023). When an attack occurs, the consequences can be devastating, such as disruption in business operations, disrupted customer service, data leakage, and violations of privacy and data protection laws. The impact of such attacks can also result in a huge waste of time and cost.

According to a report from Check Point Research, there was a 38% increase in global cyberattacks in 2022 compared to the previous year, with 83% of organizations experiencing at least one data breach in the period (Riadi et al., 2022). Based on national data from the National Cyber and Encryption Agency (BSSN), 2022 recorded 399 suspected cyber incidents, with the highest type of incident being a data breach. One prominent example is the data breach perpetrated by a hacker known as Bjorka. Cyberattacks are often triggered by weaknesses in the security of applications that can be exploited for criminal purposes. Security is a major challenge in application infrastructure due to potential threats from internal and external parties who seek to damage, steal, or modify data on the system. These threats can be viruses, malware, hacker attacks, or even information leaks from irresponsible employees (Wibowo et al., 2024).



One of the stages that can be used for security is by collecting information to identify targets, which includes information such as operating system, network topology, IP address, open ports, and DNS used. The NIST Cybersecurity Framework is considered a best practice for building a cybersecurity framework. The framework is structured around five main components identification, protection, detection, response, and recovery. Each component provides a holistic perspective on cybersecurity risk mitigation measures. By structuring these five aspects, organizations can achieve a comprehensive and structured approach to dealing with cyber challenges and threats, covering all aspects from risk recognition to recovery after incidents. NIST's cybersecurity implementation gives website managers the authority to identify and manage cybersecurity risks by assessing any existing threats.

Using this framework, you can systematically evaluate potential security risks, assign a value to threat levels, and develop appropriate protection strategies. This approach provides effective tools for website managers to design appropriate security measures and mitigate potential risks that could threaten the integrity and security of systems (Dwiyanto et al., 2023).

This research will collect information and implement several stages to produce a comprehensive report covering all aspects of the system. After that, adjustments will be made to conform to the standards set by the NIST Cybersecurity Framework. These adjustments include the integration of aspects such as resistance to cyberattacks and cyber resilience, including confidentiality, integrity, and availability. The purpose of this study is to optimize the cybersecurity framework based on NIST guidelines, so that the system can more effectively protect information and maintain the sustainability of its operations from various cyber threats (Delgado et al., 2021).

The website that was the subject of this study was *doblehost.com*, a platform for hosting providers. The presence of this website is very important because it includes quite a lot of information, so adjustments based on NIST Cybersecurity Framework guidelines are needed to be a crucial step. By implementing security standards from NIST, it is hoped that this website

will be more resistant to cyberattacks in the future. This adjustment effort aims to increase the level of security, maintain data integrity, and ensure system availability, so that the website can operate safely and efficiently (Risiko et al., 2022).

There are several studies used as review literature materials such as conducted by Tim Weil the conclusion of the study is that in the context of information technology, the pandemic has highlighted weaknesses and vulnerabilities in IT systems (Adamu et al., 2021). Therefore, cybersecurity framework standards and guidelines are needed as a reference to address the threat of cyberattacks (Balafif 2023).

The second study, conducted by Fatin Hanifah They describe the NIST Cybersecurity framework (CSF) developed by the National Institute of Cybersecurity Standards and Technology (NIST), which offers five functions to Identify, Protect, Detect, Respond and Recover from cyber threats and vulnerabilities. The solution they offer is the development of CSF webtools that provide a set of free perks, risk-based standards, and best practices to help facility owners and operators manage cybersecurity risks more effectively. Maturity evaluations in the five cybersecurity domains are determined by core assessments, and the CSF webtool allows facilities to assess their compliance with NIST's CSF as well as track security status (Hardani et al., 2022).

The third study, conducted by Mierzwa and his team, is titled "Proposed Development and Addition of a Cybersecurity Assessment Section into Technologies Involving Global Public Health". In this study, Mierzwa and colleagues propose the adoption of existing frameworks and guidelines in public health, including one of which is the NIST Cybersecurity framework. This research provides direction for global public health researchers and practitioners to include risk and vulnerability analysis in projects related to technology development and implementation (Suhartono et al., 2021).

The fourth study, conducted by Hassanzadeh and colleagues, was titled "Review of Cybersecurity Events in the Water Sector". They describe their critical evaluation of cybersecurity incidents occurring within the water and wastewater (WSS) sector, to provide protective measures against cyber threats. The solution they offer is to compile a list of the most effective



security measures that every organization should consider (Kwon et al., 2020).

The selection of the NIST Cybersecurity framework is based on the 2019 SANS OT/ICS cybersecurity survey, which shows that the framework is most widely adopted by organizations worldwide. In addition, the NIST Cybersecurity framework can help optimize time and reduce costs by providing immediate needs for the companies or organizations that use it. It is hoped that this research will help website owners in better understanding and implementing risk management, so as to reduce the likelihood of cyberattacks and minimize damage if cyberattacks occur.

## 2 Method

In this study, we will use stages related to the Nist Cybersecurity Framework. For more details, you can see in figure 1.



Figure 1. Flow Nist Cybersecurity Framework

The NIST Cybersecurity Framework is a guide developed by the National Institute of Standards and Technology (NIST) in the United States to help organizations manage and mitigate cybersecurity risks. The framework is designed to be flexible and adaptable to the needs of different types of organizations, both public and private sectors.

The NIST Cybersecurity Framework (NIST CSF) consists of five core functions: Identify, Protect, Detect, Respond, and Recover. The Identify function helps organizations understand and manage risks to their assets, data, and business capabilities. The Protect function focuses on implementing security measures to protect systems

and data. The Detect function includes the ability to detect cybersecurity events in a timely manner. The Respond function provides guidance on how to respond to cybersecurity incidents that occur. The Recover function assists in the planning and execution of recovery measures after an incident occurs. The framework is designed to be flexible and adaptable to the needs of different types of organizations, both public and private sectors, to improve their cybersecurity posture through an iterative and systematic approach.

### 2.1 Identify

In this process, the data is documented and categorized fundamentally to gather information relevant to the incident or threat. This step involves recording data sources and grouping data based on their relevance to the investigation being conducted. This process is crucial as it lays the foundation for the subsequent stages of the forensic process. By systematically documenting and categorizing data, investigators can ensure that they have a comprehensive understanding of the scope and nature of the incident (Alshar'e 2023). The identification stage may involve collecting logs, system snapshots, network traffic data, and other relevant artifacts that can provide insights into the incident.

### 2.2 Protect

This stage focuses on the development and implementation of protective measures to keep critical services and data safe. This includes using encryption, firewalls, and intrusion detection systems to protect sensitive data and critical systems from threats (Risiko et al., 2022). Protecting the integrity and confidentiality of data is paramount, as it prevents unauthorized access and mitigates the risk of data breaches. Additionally, regular updates and patches to systems and software, access control mechanisms, and security awareness training for employees are essential components of a robust protection strategy. The protect phase aims to create a secure environment that minimizes vulnerabilities and reduces the likelihood of successful attacks (Aboutabit et al., 2021).

### 2.3 Detect

The detect process aims to identify and detect suspicious activity or security threats. This

process involves monitoring networks and systems using intrusion detection tools, log analysis, and real-time monitoring to spot signs of security threats and possible risks. Early detection is critical to responding swiftly and effectively to incidents. Techniques such as anomaly detection, signature-based detection, and behavior analysis can help identify unusual patterns that may indicate a security threat (Zakaria et al., 2020). By continuously monitoring for signs of compromise, organizations can quickly detect and mitigate potential threats before they cause significant damage.

## 2.4 Respond

The response stage or fourth stage involves the preparation and execution of a rapid response to deal with an attack or security incident. This includes isolation of affected systems, data recovery, and notification to relevant parties, as well as devising strategies to prevent further spread of threats. Effective incident response requires a well-defined plan that outlines roles, responsibilities, and procedures to follow in the event of an incident. The goal is to contain the threat, minimize impact, and restore normal operations as quickly as possible (Hansen et al. 2023). Communication with stakeholders, including customers, employees, and regulatory bodies, is also a critical component of the response phase. By having a clear and practiced response plan, organizations can reduce downtime and recover more efficiently from security incidents.

## 2.5 Recover

This stage includes long-term planning to recover assets that may have been lost due to the incident and ensure operations return to normal. This step involves developing a recovery plan, restoring data from backups, repairing broken systems, and reevaluating security policies to improve resilience to future incidents (Nassar and Kamal 2021). Recovery is not just about restoring systems to their previous state but also about learning from the incident to enhance future security measures. This may involve conducting a post-incident review to identify lessons learned, updating incident response plans, and implementing additional safeguards to prevent similar incidents in the future. The combination of these five stages forms a comprehensive forensic

process, which ensures security threats can be effectively identified, dealt with, and prevented.

Then for the plan used in this study, it is carried out at the beginning of the study where the researcher targets which web to use then continues to conduct research on the web.

## 3 Results

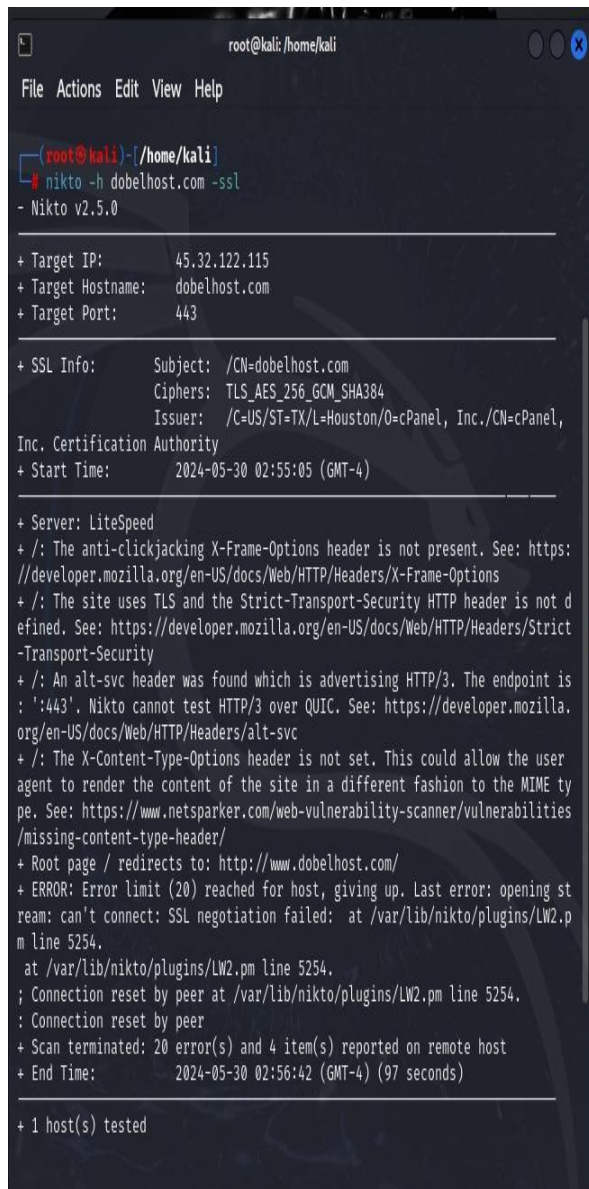
### 3.1 Server Checking

In this study, the command 'nikto -h dobelhost.com -ssl' was used to perform a thorough security check on the web server 'dobelhost.com' using the HTTPS protocol. Nikto, as a widely recognized open-source web server scanning tool, is designed to detect potential vulnerabilities and misconfigurations on web servers. This check targets IP 45.32.122.115 on port 443 with the target hostname dobelhost.com. The SSL information found includes the subject /CN=dobelhost.com, cipher TLS\_AES\_256\_GCM\_SHA384, and issuer /C=US/ST=TX/L=Houston/O=cPanel, Inc./CN=cPanel, Inc. Certification Authority, with the certificate start time on 2024-05-30 02:55:05 (GMT-4).

The results of the check showed that the server was using LiteSpeed. Some of the vulnerabilities found include the absence of the X-Frame-Options Anti-Clickjacking header, which could lead to clickjacking attacks, as well as the undetected Strict-Transport-Security, which could lead to unprotected data if sent over HTTP. The Alt-Svc header was found to advertise HTTP/3 with endpoints using "h3" and HTTP/1.1. Additionally, the X-Content-Type-Options header is not set, which could allow attackers to render content in a different form than intended.

The check also showed several technical errors, including a failed SSL negotiation error, which was logged in /var/lib/nikto/plugins/PLUGINS.pm line 5254. The scan is performed for 97 seconds and stops after reaching the error limit (20) for the host. By addressing these findings, 'dobelhost.com' administrators can significantly improve the security of their servers, help prevent cyberattacks, and ensure better protection of the data and services provided. The results of the detailed server check can be seen in figure 2.





```
root@kali: /home/kali
File Actions Edit View Help

(root@kali) - /home/kali
# nikto -h dobelhost.com -ssl
- Nikto v2.5.0

+ Target IP: 45.32.122.115
+ Target Hostname: dobelhost.com
+ Target Port: 443

+ SSL Info: Subject: /CN=dobelhost.com
           Ciphers: TLS_AES_256_GCM_SHA384
           Issuer: /C=US/ST=TX/L=Houston/O=cPanel, Inc./CN=cPanel,
Inc. Certification Authority
+ Start Time: 2024-05-30 02:55:05 (GMT-4)

+ Server: LiteSpeed
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: http://www.dobelhost.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: at /var/lib/nikto/plugins/LW2.pm line 5254.
at /var/lib/nikto/plugins/LW2.pm line 5254.
; Connection reset by peer at /var/lib/nikto/plugins/LW2.pm line 5254.
; Connection reset by peer
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time: 2024-05-30 02:56:42 (GMT-4) (97 seconds)

+ 1 host(s) tested
```

Figure 2. Server Checking

### 3.2 Scan Ip Dns

In this study, the 'nslookup dobelhost.com' command was used to check the DNS information of the 'dobelhost.com' domain. This command makes it possible to identify the IP address associated with the 'dobelhost.com' as well as the responsible DNS server. This information is particularly useful for network connectivity troubleshooting, allowing administrators to detect and resolve issues that may occur with DNS resolution or other network configurations. When the 'nslookup' command is executed, the system sends a request to the DNS server configured on the local device to look for information related to

'dobelhost.com'. The results include the IP address associated with the domain as well as information about the DNS server that responded to the request.

The IP address found indicates the location and identity of the server hosting the 'dobelhost.com' domain, which helps in identifying the source of the problem in case of a service outage or targeted attack on that server. Information regarding the DNS server responsible provides additional insight into the DNS structure and management of the domain, which can be key in identifying name resolution issues or if any changes need to be made to the DNS configuration. The data obtained from 'nslookup' is crucial in network troubleshooting, as if there is a problem with DNS resolution, administrators can use this information to evaluate whether the problem is coming from the DNS server, network configuration, or other factors.

### 3.3 Scan Ip Port

To perform IP and port scans using the nmap application, the 'nmap dobelhost.com' command is used. This command checks the IP address associated with the domain and identifies the open ports as well as the services running on the server. The results of these scans help in detecting potential vulnerabilities and improving network security. When the 'nmap dobelhost.com' command is executed, nmap sends a request to the server to check the status of the port and the running service. The scan results showed that the IP address 45.32.122.115 was connected with 'dobelhost.com' and the host was detected to be active with a latency of 0.023s. The rDNS record for 45.32.122.115 indicates that the associated host is home2023sg.colorado.com.

The scan identified several open ports and services running on those servers, including ports 21 (FTP), 25 (SMTP), 53 (DNS), 80 (HTTP), 110 (POP3), 143 (IMAP), 443 (HTTPS), 465 (SMTPS), 587 (Submission), 993 (IMAPS), and 995 (POP3S). In addition, there are 989 TCP ports that are filtered and do not respond.

These results indicate that the server has some critical services running and open ports. Identification of these ports is important to understand the attack surface that may be present on the server. Administrators can use this information to secure ports and services that are not needed and ensure that running services are



updated and configured correctly to reduce the risk of vulnerabilities. Figure 3 displays the results of the IP and port scans in detail, providing a visual overview of the security status of the 'dobelhost.com' server network. The scan was completed in 6.80 seconds, demonstrating the efficiency and speed of the nmap tool in doing its job.

```
(root@kali)~/home/kali
└─$ nmap dobelhost.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-30 03:01 EDT
Nmap scan report for dobelhost.com (45.32.122.115)
Host is up (0.023s latency).
rDNS record for 45.32.122.115: home2023sg.colorado.id
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 6.80 seconds
```

Figure 3. Result of Scan IP Port

### 3.4 Penetration Testing

The command 'nmap -v -A -sV dobelhost.com' is used to perform a deep scan of the 'dobelhost.com' server with a high level of detail. The '-v' option enables verbose mode to provide more detailed output, '-A' allows detection of the operating system, service version, and scanning scripts, while '-sV' specifically checks the version of the service running on an open port. These scans provide comprehensive insights into server configurations, services running, and their potential vulnerabilities, which is very beneficial for improving security and identifying areas that require further attention.

In this website there is very little vulnerability but it would be better to stay on guard – just keep hacking from happening. Details of website testing can be seen in figure 4.

```
(root@kali)~/home/kali
└─$ nmap -v -A -sV dobelhost.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-30 03:24 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:24
Completed NSE at 03:24, 0.00s elapsed
Initiating NSE at 03:24
Completed NSE at 03:24, 0.00s elapsed
Initiating NSE at 03:24
Completed NSE at 03:24, 0.00s elapsed
Initiating Ping Scan at 03:24
Scanning dobelhost.com (45.32.122.115) [4 ports]
Completed Ping Scan at 03:24, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:24
Completed Parallel DNS resolution of 1 host. at 03:24, 5.23s elapsed
Initiating SYN Stealth Scan at 03:24
Scanning dobelhost.com (45.32.122.115) [1000 ports]
Discovered open port 21/tcp on 45.32.122.115
Discovered open port 993/tcp on 45.32.122.115
Discovered open port 443/tcp on 45.32.122.115
Discovered open port 25/tcp on 45.32.122.115
Discovered open port 53/tcp on 45.32.122.115
Discovered open port 587/tcp on 45.32.122.115
Discovered open port 143/tcp on 45.32.122.115
Discovered open port 995/tcp on 45.32.122.115
Discovered open port 110/tcp on 45.32.122.115
Discovered open port 80/tcp on 45.32.122.115
Discovered open port 465/tcp on 45.32.122.115
Completed SYN Stealth Scan at 03:24, 5.77s elapsed (1000 total ports)
Initiating Service scan at 03:24
Scanning 11 services on dobelhost.com (45.32.122.115)
Completed Service scan at 03:24, 41.68s elapsed (11 services on 1 host)
Initiating OS detection (try #1) against dobelhost.com (45.32.122.115)
Retrying OS detection (try #2) against dobelhost.com (45.32.122.115)
Initiating Traceroute at 03:25
Completed Traceroute at 03:25, 0.06s elapsed
Initiating Parallel DNS resolution of 1 host. at 03:25
Completed Parallel DNS resolution of 1 host. at 03:25, 0.02s elapsed
NSE: Script scanning 45.32.122.115.
Initiating NSE at 03:25
Completed NSE at 03:25, 24.21s elapsed
Initiating NSE at 03:25
NSE Timing: About 88.64% done; ETC: 03:29 (0:00:30 remaining)
NSE Timing: About 90.91% done; ETC: 03:30 (0:00:30 remaining)
NSE Timing: About 92.05% done; ETC: 03:31 (0:00:30 remaining)
NSE Timing: About 93.18% done; ETC: 03:32 (0:00:30 remaining)
```

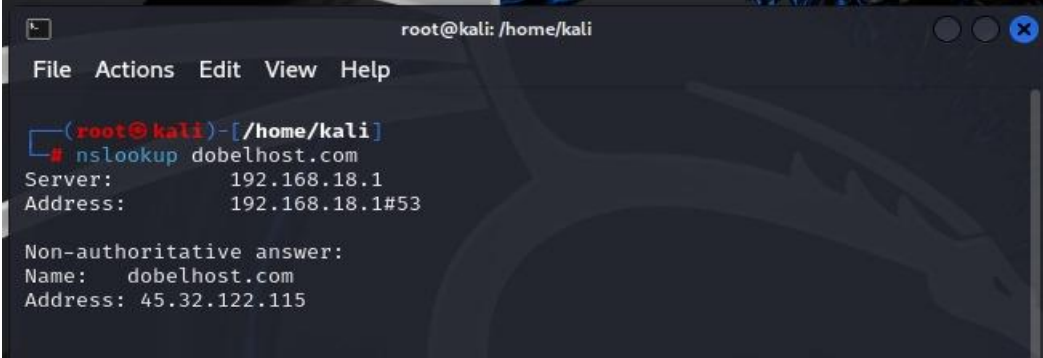
Figure 4. Result of Testing

### 3.5 NSlookup

The 'nslookup dobelhost.com' command is used to get DNS information related to that domain. By executing this command, we can find the IP address connected to the 'dobelhost.com' and identify the DNS server responsible for this domain. The data obtained through 'nslookup' is very useful for network connectivity troubleshooting, helping to detect and resolve potential problems in DNS resolution or network configuration. The results of this command show that the DNS server used is at the IP address 192.168.18.1 and port 53, which is usually a local DNS server or one configured in the network

settings. In addition, the non-authoritative results show that the IP address connected to 'dobelhost.com' is 45.32.122.115, which means this information is obtained from the cache and not directly from the authoritative DNS server for the domain. These commands and their results are very

useful for verifying that DNS resolution is working correctly and helping to identify if there are problems with the DNS server configuration or connectivity between the client and the DNS server. For the results of the ip and NSLOOKUP details can be seen in figure 5.



```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[~/home/kali]
└─# nslookup dobelhost.com
Server:          192.168.18.1
Address:         192.168.18.1#53

Non-authoritative answer:
Name:   dobelhost.com
Address: 45.32.122.115
```

Figure 5. Result NSLOOKUP

#### 4 Conclusion

After doing various checks ranging from checking servers, ip scans and alinnya it can be concluded that with this research it is expected that all website owners know how important the security of a website is and must know more details related to IP Address and others. So that cyber resilience can be strengthened and resistance to cyberattacks can be built. Currently, the specific contribution of information collection to the security of dobelhost.com website is as information collection allows the identification of early vulnerabilities in the system, such as misconfigurations and security holes that can be exploited by attackers. By knowing potential weak points, corrective steps can be taken immediately. The information collection process increases the awareness of the website management team to existing threats, including understanding the operating system used, network topology, IP address, open ports, and DNS used. Based on the information obtained, UPT Sistem Informasi can regularly perform software updates and system maintenance to close security gaps found and reduce the risk of cyberattacks. Knowing the potential for possible attacks, teams can develop better and faster incident response procedures, so as to minimize the impact of cyberattacks. In addition, the information collected assists in the more precise application of the security standards of the NIST Cybersecurity Framework, ensuring

that all aspects of the framework are effectively implemented.

#### References

- Alshar'e, Marwan. 2023. "Cyber Security Framework Selection: Comparision of Nist and Iso27001." *Applied Computing Journal* 245–55. Doi: 10.52098/Acj.202364.
- Balafif, Sabri. 2023. "Penyesuaian Model Ketahanan Siber Umkm Di Indonesia Dengan Nist Cybersecurity Framework." 8(3).
- Dwiyanto, Arif Rifai. 2023. "Prevalensi Penerapan Rfc 9116 Untuk Membantu Pengungkapan Kerentanan Keamanan Siber Di Perguruan Tinggi Indonesia." 1(2). Doi: 10.38035/Jgit.V1i2.
- Frayssinet Delgado, Maurice, Doris Esenarro, Francisco Fernando Juárez Regalado, And Mónica Díaz Reátegui. 2021. "Methodology Based on The Nist Cybersecurity Framework as A Proposal for Cybersecurity Management in Government Organizations." *3c Tic: Cuadernos De Desarrollo Aplicados A Las Tic* 10(2):123–41. Doi: 10.17993/3ctic.2021.102.123-141.
- Garba, Adamu Abdullahi, Aliyu Musa Bade, Adamu A Garba, And Aliyu M. Bade. 2021. *An Investigation on Recent Cyber Security Frameworks as Guidelines for Organizations Adoption*. Vol. 6.
- Hansen, Jerry, Tata Sutabri, Universitas Bina Darma Palembang, And Histori Artikel. 2023. "Mendesain Cyber Security Untuk Mencegah Serangan Ddos Pada Website Menggunakan Metode Captcha." *Digital Transformation*



- Technology (Digitech) / E* 3(1). Doi: 10.47709/Digitech.V3i1.2764.
- Hardani, Muhammad Salmon, And Kalamullah Ramli. 2022. "Perancangan Manajemen Risiko Keamanan Sistem Informasi Manajemen Sumber Daya Dan Perangkat Pos Dan Informatika (Sims) Menggunakan Metode Nist 800-30." *Jurikom (Jurnal Riset Komputer)* 9(3):591. Doi: 10.30865/Jurikom.V9i3.4181.
- Ilmu Komputer, Jurnal, Sistem Informasi, And Teknik Informatika. 2024. *Tinjauan Implementasi National Institute of Standards and Technology (Nist) Dalam Meningkatkan Keamanan Jaringan Dengan Cybersecurity Framework (Csf): Studi Kasus Smkn4 Bandar Lampung*. Vol. 3.
- Kwon, Roger, Travis Ashley, Jerry Castleberry, Penny Mckenzie, And Sri Nikhil Gupta Gouriseti. 2020. "Cyber Threat Dictionary Using Mitre Attck Matrix and Nist Cybersecurity Framework Mapping." Pp. 106–12 In *2020 Resilience Week, Rws 2020*. Institute Of Electrical and Electronics Engineers Inc.
- Nassar, Ahmed, And Mostafa Kamal. 2021. *Machine Learning and Big Data Analytics for Cybersecurity Threat Detection: A Holistic Review of Techniques and Case Studies*.
- Perpustakaan Daerah Provinsi Sumatera Selatan, Pada, Cristian Renaldi Simanjuntak, Syahreza Akbar Pratama, Guntoro Barovich, And Institut Teknologi Dan Bisnis Palcomtech. 2023. *Remanajemen Jaringan Menggunakan Framework Nist Network Remanagement Using the Nist Framework ast The Regional Library of South Sumatra Province*. Vol. 4.
- Riadi, Imam. 2022. "Analisis Forensik Smartphone Android Menggunakan Metode Nist Dan Tool Moleedit Forensic Express."
- Risiko, Manajemen, Serangan Siber, Tony Tan, And Benfano Soewito. 2022a. "Ciptaan Disebarluaskan Di Bawah Lisensi Creative Commons Atribusi 4.0 Internasional." *Journal Of Information System, Applied, Management, Accounting and Research* 6(2):411–22. Doi: 10.52362/Jisamar.V6i2.781.
- Risiko, Manajemen, Serangan Siber, Tony Tan, And Benfano Soewito. 2022. "Ciptaan Disebarluaskan Di Bawah Lisensi Creative Commons Atribusi 4.0 Internasional." *Journal Of Information System, Applied, Management, Accounting and Research* 6(2):411–22. Doi: 10.52362/Jisamar.V6i2.781.
- Suhartono, Didit, And Khairunnisak Nur Isnaini. 2021. "Strategi Recovery Plan Teknologi Informasi Di Perguruan Tinggi Menggunakan Framework Nist Sp 800-34." *Matrik: Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer* 20(2):261–72. Doi: 10.30812/Matrik.V20i2.1097.
- Sulistyowati, Diah, Fitri Handayani, And Yohan Suryanto. N.D. *Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using Nist Csf, Cobit, Iso/Iec 27002 And Pci Dss*.
- Surono Wibowo, Dega, Taufiq Abidin, Jurusan Teknik Informatika, Politeknik Harapan Bersama, And Jln Mataram No. 2024. "Pengumpulan Informasi Pada Situs Web Dengan Menyusun Kerangka Kerja Keamanan Siber Nist." 9(1).
- Syafrizal, Melwin, Siti Rahayu Selamat, And Nurul Azma Zakaria. 2020. *Analysis of Cybersecurity Standard and Framework Components*. Vol. 12.
- Tissir, Najat, Said El Kafhali, And Nouredine Aboutabit. 2021. "Cybersecurity Management in Cloud Computing: Semantic Literature Review and Conceptual Framework Proposal." *Journal Of Reliable Intelligent Environments* 7(2):69–84.