PLAGIARISM CHECK.ORG

70.71% SIMILARITY OVERALL

6.14% POTENTIALLY AI

SCANNED ON: 16 FEB 2025, 5:05 PM

Similarity report

Your text is highlighted according to the matched content in the results above.

IDENTICAL 5.18%

CHANGED TEXT 65.52%

REFERENCES 1.54%

AI Detector Results

Highlighted sentences with the lowest perplexity, most likely generated by AI.

LIKELY AI 5.13%

HIGHLY LIKELY AI 1.01%

Report #24825067

1 2 3 4 5 6 7 8 9 10 11 13 14 15 16 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 149 151 152 153 155 156 157 158 160 161 162 164 165 167 172 177 210 -299720-421450 00 20383506000750INTERNATIONAL SCHOOL OF MANAGEMENT AND TECHNOLOGY FACULTY OF COMPUTING ASSIGNMENT COVER SHEET This form is to be completed by students submitting assignments of level 4 and level 5. 1 2 3 4 5 6 7 8 9 10 11 13 14 15 16 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 149 151 152 153 156 158 160 161 164 167 172 177 210 Students are required to complete all sections and attach to your assignment. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125

126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 155 156 157 158 159 160 161 162 163 164 165 166 167 172 177 STUDENT DETAILS STUDENT NAME VANSH SHARMA STUDENT ID BUT2023ITB003 UNIT AND ASSIGNMENT DETAILS UNIT TITLE Unit 29: Network Security UNIT NUMBER M/618/7443 ASSIGNMENT TITLE Nobel College Security ISSUE DATE December 17, 2024 DUE DATE February 16, 2025 ASSESSOR NAME Aashish Pandey ESTIMATED WORD LENGTH 16000 SUBMISSION HAND IN DATE February 16, 2025 DECLERATION AND ACKNOWLEDGEMENT When submitting assignments, each student must sign a declaration confirming that the work is their own. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 155 157 158 159 162 163 165 168 Plagiarism and Collusion Plagiarism: to use or pass off as one’s own, the writings or ideas of another without acknowledging or crediting the source from which the ideas are taken. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 Collusion: submitting an assignment, project or report completed by another person and passing it off as one’s. In accordance with the Academic Integrity and Plagiarism Policy: I declare that: this assignment is entirely my own work, except where I have included fully-documented references to the work of others, the material contained in this assignment has not previously been

submitted for any other subject at the University or any other educational institution, except as otherwise permitted, no part of this assignment or product has been submitted by me in another (previous or current) assessment, except where appropriately referenced, and with prior permission from the Lecturer / Tutor / Unit Coordinator for this unit. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 161 162 163 164 165 166 167 168 211 I acknowledge that: if required to do so, I will provide an electronic copy of this assignment to the assessor; 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 166 168 168 211 the assessor of this assignment may, for the purpose of assessing this assignment: reproduce this assignment and provide a copy to another member of academic staff; 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 166 168 communicate a copy of this assignment to a plagiarism checking service such as Plagiarism Check (which may then retain a copy

of this assignment on its database for the purpose of future plagiarism checking).
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61
62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90
91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114
115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 133 134 135 136 137
138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 156 157 159 160 161
163 166 167 168 I am aware of and understand that any breaches to the Academic Code of Conduct will be investigated and sanctioned in accordance with the College Policy. 1 4 5 6 7 11 18 21 23 24 27 29 32
33 34 38 40 43 44 47 50 52 54 55 56 57 58 65 66 68 75 81 86 87 89 90 92 93 97 102 103
104 111 114 115 117 118 123 128 131 138 154 159 SIGNATURE VANSH SHARMA DATE February 16, 2025 Contents Introduction:7P1 Discuss the different types of Network Security devices. 7Network Security7Core Network Security Principles9Types of Network Security Devices111. Firewalls112. 1 7 11 20
25 31 43 52 72 143 176 233 Intrusion Detection and Prevention Systems (IDPS)123.
1 7 10 11 20 22 25 43 52 72 118 143 176 233 Virtual Private Network (VPN) Devices134. 1 7 10 11 20 22 25 43 52 72 118 176 Network Access Control (NAC) Devices145. 1 20 25 43 52 72 176 Anti-Malware and Antivirus Solutions156. Load Balancers167. 1 4 20 52 Data Loss Prevention (DLP) Systems16P2 Examine network security protocols and the use of different cryptographic types in network security. 1 17Security Protocols17SSL/TLS (Secure Sockets Layer / Transport Laye r Security)17SHTTP (Secure Hypertext Transfer Protocol)19SET (Secure Electronic Transaction)19PEM (Privacy-Enhanced Mail)20PGP (Pretty Good Privacy)21PPTP (Point-to-Point Tunneling Protocol)22Cryptography23Hashing26Digital Signature28Cybersecurity Standards29ISO 27000 Series30NIST SP 800-5331NIST SP 800-17132NIST Cybersecurity Framework (CSF)34NIST SP 1800 Series36OWASP (2021)36MITRE37M1 Compare and contrast at least two major Network Security protocols. 38SSL/TLS38IPsec (Internet Protocol Security)39SSH

(Secure Shell)39Comparison of SSL/TLS, IPsec, and SSH40Table Summary40Reason for Choosing Specific Protocols41Justification for Protocol Selection41Difference in Network Security Before and After Using the Protocols41Conclusion42D1 Evaluate the importance of network security to an organization. 42Introduction422. Importance of Network Security423. Critical Network Security Components454. 1 4 29 30 38 44 171 193 212 Conclusion47P3 Investigate the purpose and requirements of a secure network according to a given scenario. 47Building a Secure Network Infrastructure47Security Planning at Nobel College47a. 1 Next-Generation Firewall (NGFW)47Intrusion Detection and Prevention System (IDPS)48c. Virtual Private Network (VPN)48d. Endpoint Security49e. 1 7 67 68 69 128 233 252 Security Information and Event Management (SIEM)49g. 1 233 252 Network Access Control (NAC)502. 1 Purpose of a Secured Network513. Things to be Protected51P4 Determine which network hardware and software to use in this network. 52Network Hardware521. Switches522. Multilayer Switch533. Router544. Firewall545. Access Points556. Servers56Network Software571. Network Operating System (NOS)572. Network Configuration and Management Software573. Network Security Software584. Networking Protocol Software585. 1 Cloud Networking and Virtualization Software596. 1 Network Communication Software59How Hardware and Software Work Together to Improve Network Security60M2 Create a design of a secure network according to a given scenario. 61Network Design of Nobel College61Key Components in the Network621. Router622. Physical Firewall623. Multilayer Switch624. Access Layer Switches (3)625. Servers (4)636. End-User PCs (6)63Limitations of the Current Network Design63Network Summary63Enhanced Network Design64Key Enhancement:64Comparison Table: Current vs. Enhanced Network Design66Justification for Using Multiple Devices66Conclusion66P5 and M3:67Network Design Explanation67Devices and Configuration Overview68Switches:68Multilayer Switch71Configuring the Servers.85DNS85Print Server88File Server89Database Server:92Why use cloud? Reasoning:93Quality

of Service (QoS):93Syslog95P6: Comprehensively test your network using the devised Test Plan.971. Introduction to the Test Plan and Its Importance972. Identification97Objectives97ii. Test Scenarios98iii. Test Cases98Test Plan Table99Why cannot we use VPN?100Test Cases with Verification100Connectivity Test100VLAN and Inter-VLAN Connectivity Test103Firewall Test107ACL Test109Servers Test112IP address table115DHCP has been used to asign IP addresses.116M4 - Analysis of Test Results and Recommendations for Network Enhancements1161. Physical and IP Connectivity Tests1162. VLAN and Inter-VLAN Connectivity Tests117Summary119D2: Critical Evaluation of the Network Design, Planning, Configuration, and Testing119Introduction1191. Design & Planning Assessment1202. Configuration Evaluation1213. Testing Evaluation1225. Overall Assessment125Appendix:126Presentation:126References:129
Figure 1 Network Security9Figure 2 Network Security Principles10Figure 3 : Firewall12Figure 4 Intrusion Detection System13Figure 5 Virtual Private Network15Figure 6 Load Balancers17Figure 7 TLS/SSL19Figure 8 PEM21Figure 9 PGP22Figure 10 PPTP23Figure 11 Cryptography24Figure 12 Symmetric Encryption25Figure 13 Asymmetric Encryption26Figure 14 Hashing28Figure 15 Digital Signature29Figure 16 ISO 27000 SERIES31Figure 17 NIST SP 800-5332Figure 18 NIST SP 800-17134Figure 19 NIST CSF36Figure 20Switch54Figure 21 Multilayer Switch54Figure 22 Router55Figure 23 Firewall56Figure 24 Server57Figure 25 : Initial Design of the Network62Figure 26 Secure Network Design for Nobel College68Figure 27 Ping Successful102Figure 28 Ping Unsuccessful103Figure 29 Inter-VLAN Test104Figure 30 DHCP Request Successful106Figure 31 HSRP Test107Figure 32 Firewall doesn’t allow unauthorized traffic109Figure 33 Firewall allows authorized traffic110Figure 34 : Specified devices communicate111Figure 35 Unspecified devices don't communicate112Figure 36 DNS accessed by using domain114Figure 37 Print server accessed115Figure 38 File server accessed115

Introduction: The Nobel College, the most prestigious educational institution in the entire world which is renowned for its quality in both research and technological programs, has engaged me in the process of security upgrading, By implementing robust security measures, I aim to enhance data protection, improve operational efficiency, and ensure the educated attackers who use evolving cyber threats to target the college will not succeed.
The college is a large community with its students and staff who are confronted with sensitive data processing the issues of large quantities of data no small part of which includes personal student records, research materials, and many other confidential information. The College authorities have been bombarded by the Information Security team with several reported issues like unauthorized network access and data breaches as a result of failure to protect the college digital assets. My specific task is to figure out the major weaknesses of the college's network infrastructure and then to reinforce the weak spots in the existing network, thus making it more impregnable against the potential threats. This job entails studying the current network topology and finding out which firewall configurations are very efficient along with inspecting how the institution's intrusion detection systems (IDS) are performing. Furthermore, I will study previous security breaches to find out possible causes, e.g. unauthorized access, data breaches, or possible threats of cyber. 1 9 18 19 30 35 38 74 112 123 175 183 185 212 P1 Discuss the different types of Network Security devices. Network Security Network security is the process of implementing various set of protocols, solutions, rules, and technologies whose aim is to make sure the integrity, confidentiality, and availability of network and data is preserved. It is a set of rules and regulations that are used to protect network infrastructure from unauthorized access, data

breaches, and other forms of cyberattacks. (Stallings, 2017) Figure 1 Network Security What is Network Security? Defends hardware from a multitude of cyber threats, such as malware, ransomware, and other hacking attempts. Safely stores information by not allowing anyone except authorized persons to have access to the information, thus securing it from unauthorized access. Network continuity can be backed up by organizations in the case of security incidents creating less downtime. 1 4 It helps to get the trust of the customer by creating a secure workspace or environment for both customers and stakeholders while also improving data privacy and system security. 4 Network Security Basic Principles Enterprises actualize network security methodologies based on the significant principles which are the core of the overall protection. 1 4 Core Network Security Principles Figure 2 Network Security Principles 1. Confidentiality Sensitive data should be exclusively for people who are authorized. Passwords and financial transactions are kept absolutely safe from all forbidden access by encryption techniques. 2.Integrity To prevent any modifications that are not allowed, all systems have to make sure every piece of data stays correct and logical. 1 Hashing algorithms, for example SHA-256, help verify data integrity. 1 3.Availability Those people who have permission should consistently be able to obtain network resources, as is required. Because they spread traffic out well, load balancers help stop servers from failing. 1 4 4.Authentication Each user must confirm identity to get any network resources. 1 4 250 Multi-factor authentication (MFA) needs both a password and biometric verification. 1 4 5.Authorization Every system has to give each user permission according to roles and responsibilities. 1 4 9 14 18 23 24 32 40 58 60 61 66 75 101 108 113 114 146 169 170 174 194 209 220 247 Role-Based Access Control (RBAC) restricts every access to cloud services based on all user roles. 6.Non-Repudiation Guarantees each network action can be traced back to the users who are responsible. Digital signatures verify

that emails are real as well as that transactions are real. 7.Least Privilege Only allow users and systems the access required for their tasks. Employee access should be limited to files connected to the employee's department. 8.Defense in Depth Several security steps should be used to protect everything that makes up the network. [1] Working together, multiple firewalls, antivirus software programs and intrusion detection systems offer improved security. (Stallings, 2017) (Kizza, 2020)Network Security Devices Network security devices consist of hardware and software solutions designed to monitor, regulate, and protect network data flow from potential threats Types of Network Security Devices 1. [4] [7] [11] Firewalls Purpose: Firewalls enforce security policies by filtering network traffic, ensuring internal systems are safeguarded from external threats while maintaining a secure network perimeter. [2] [3] Figure 3 : Firewall Functionality: Examines incoming and outgoing data packets. [119] [219] Allows or blocks network traffic based on predefined rules. [2] [3] [4] Operates across multiple OSI layers, including Network, Transport, and Application layers. [1] [2] [3] [4] [95] [115] Types: Stateful Inspection Firewall: Monitors active connections and their security state. [1] [14] [15] [95] Proxy Firewall: Serves as an intermediary to filter network requests. [1] [2] [3] [4] [14] [15] [27] [95] [182] [196] Next-Generation Firewall (NGFW): Integrates deep packet inspection, intrusion detection/prevention, and application-layer monitoring. [1] [2] [3] [4] [14] [15] [26] [33] [71] [102] [154] [174] [219] [245] Examples: Cisco ASA, Palo Alto Networks, Fortinet FortiGate. [1] [2] [3] [4] [14] [15] Use Cases: Securing enterprise networks. [1] [2] [3] [4] Protecting data centers and cloud applications. Preventing unauthorized network access. (Netwrix, 2019)2. [1] [18] [19] [33] [35] [71] [85] [97] [99] [108] [109] [132] [134] [183] [188] [189] [190] [238] Intrusion Detection and Prevention Systems (IDPS) Purpose: IDPS solutions analyze network activity in real-time to detect and mitigate potential threats. [1] Figure 4 Intrusion Detection System Functionality: Analyzes network traffic to detect malicious activities. IDS (Intrusion Detection System): Generates

alerts for potential threats. IPS (Intrusion Prevention System): Actively blocks detected threats. [1][2][3][4] Types: Network-based IDPS (NIDS/NIPS): Monitors traffic across an entire network. Host-based IDPS (HIDS/HIPS): Protects individual devices from threats. [1][2][3][4][214][216][245] Examples: Snort, Suricata, Cisco Firepower. [1] Use Cases: •Preventing malware attacks. •Mitigating denial-of-service (DoS) incidents. •Detecting unauthorized access attempts. (Scarfone, 2007)3. [1][2][3][4][62] Virtual Private Network (VPN) Devices Purpose: When installed through VPN solutions data transmission becomes encrypted for remote security connectivity. [4] Figure 5 Virtual Private Network Virtual Private Network (VPN) Functionality: [4] The VPN service builds an encrypted line between users and their network destinations. [2][3][4][39][59] The encryption standards of IPSec and SSL/TLS and OpenVPN are used by this system. [1][2][3][4] Types: Remote Access VPN: Enables secure access for remote employees. [1][2][3][4] Site-to-Site VPN: Connects multiple office locations securely. [1][2][3][4][36] Examples: Cisco AnyConnect, OpenVPN, NordVPN Business. [4] Use Cases: All traffic for distant workers should be protected by robust communication channels. [2][3] The protection of connections remains possible on public Wi-Fi networks which lack security. [1][2][3][4][13][20][63][154][195] 4.Network Access Control (NAC) Devices Purpose: The security policy defines how NAC solutions determine what devices can use the network. [1][2][3][4] Functionality: The system verifies and authenticates devices to determine device access permission. [1][4] Types: Before entering the network the device security compliance undergoes assessment through the pre-admission NAC process. The system performs ongoing security threat detection of devices which remain attached to the network after approval. [1][2][3][4][14][15][36][131][149][154] Examples: Cisco ISE, Aruba ClearPass. [2][3][4] Use Cases: Enforcing security policies within organizations. The network safeguards itself against unauthorized devices attempting to access its infrastructure. (Scarfone,

2007)5. 1 Anti-Malware and Antivirus Solutions Purpose: These solutions have been created to both spot and get rid of malware files while stopping new infections. Functionality: Identity threats using both behavioral patterns and established signatures to conduct appropriate threat detection. 1 2 3 4 36 Examples: McAfee, Symantec, Bitdefender. 1 Use Cases: The solutions defend computers against ransomware and numerous kinds of malware. 1 The system protects file transfers against malicious software through security measures. (Scarfone, 2007)6. 1 Load Balancers Purpose: Load Balancers guarantee network performance improvement and security through redirection of traffic across various servers. 1 2 3 4 Figure 6 Load Balancers Load Balancers Functionality: The system makes use of Round Robin and Least Connections as networking algorithms to achieve efficient traffic distribution. Types: Physical traffic distribution appliances known as hardware load balancers dedicate themselves to distributing network traffic. 1 2 3 Software Load Balancers: Virtualized solutions for flexible deployment. 1 2 3 4 Hardware Load Balancers: Physical network appliances dedicated to traffic distribution Examples:F5 BIG-IP, AWS Elastic Load Balancer (ELB). 1 2 3 4 Use Cases: The system prevents server overload which results in optimal performance. 1 4 Load balancers increase system resistance against distributed denial-of-service (DDoS) attack threats. (Stallings, 2017) (Zenarmor, 2023)7. 1 4 5 27 70 82 86 120 186 204 209 218 Data Loss Prevention (DLP) Systems Purpose: The purpose of DLP solutions helps to stop unauthorized access attempts along with preventing the unauthorized sharing and transfer of sensitive data. 1 4 Functionality:The system performs data leak checks through content analysis and contextual analysis methods. 1 2 3 4 Examples:Symantec DLP, Forcepoint DLP. Use Cases: Data Protection systems stop sensitive information from getting exposed illegally. 147 Our organization maintains GDPR and HIPAA data protection compliance through proper measures. Conclusion

Today's organizations require powerful network security systems to fight against increasing cyber dangers in their environments. [1][2][3][4] Security frameworks require multiple protection elements to function properly which includes firewalls along with IDPS, VPNs and NAC solutions and anti-malware software along with load balancers and DLP systems. The protection of data confidentiality along with continuous business operations and regulatory adherence and user trust rely on strengthened network security measures. Climbing cyberattacks sophistication requires companies to implement comprehensive security layers as an effective method for defending digital resources. [1][4][9][30][38][171][175][178][183][193] P2 Examine network security protocols and the use of different cryptographic types in network security. [1][2][3][23] Security Protocols Security protocols serve as standardized methods which defend data transmission through properties of confidentiality integrity and authentication. [2] Security protocols protect data transfers through cryptographic methods that block unauthorized modification as well as stop unauthorized access and secret exposures. [1][2][3] SSL/TLS alongside SHTTP and SET protocols together with PEM and PGP and PPTP comprise some established security protocols used for data protection. [1][2][3][5][8][9][12][17][19][29][31][33][34][41][48][56][60][65][66][67][85][91][93][101][106][107][126][148][155][169][170][171][172][173][175][178][181][182][184][185][190][192][194][197][201][203][216][226] SSL/TLS (Secure Sockets Layer / Transport Layer Security) Secure Socket s Layer and its successor Transport Layer Security constitute SSL/TLS as an encryption protocol pair. [1] Over networks and specifically on the internet SSL along with TLS serves as encryption protocols to secure data communication. TLS provides advanced encryption capacities through its extension of SSL to establish secure transmission channels and maintain integrity together with authenticity for client-server communication. Figure 7 TLS/SSL How It Works: SSL/TLS enables a secure connection through asymmetric encryption at authentication followed by the deployment of speedier

symmetric encryption for maintaining ongoing data exchange. 1 4 Digital certificates along with the generation of a specific session key establish encrypted communication through the handshake procedure. 1 2 3 4 49 104 135 173 182 Authenticity is secured by Certificate Authorities (CAs) who issue certificates that protect against both listening attacks and data tampering. 1 4 Examples & Applications: HTTPS – Secure we b browsing FTPS – Secure file transfers SMTPS – Email encryption The security protocols are crucial for establishing encryption during exchanges like emails through virtual private networks together with bank transactions. (Kizza, 2020)SHTTP (Secure Hypertext Transfer Protocol) The SHTTP protocol for HTTP adds message encryption together with authentication features but functions differently from HTTPS which secures complete sessions. 1 The encryption system of SHTTP enables several protection technologies which maintain data confidentiality and protects data integrity. 1 4 How It Works: Each transmitted HTTP message through SHTTP gains two-layer protection by applying asymmetric cryptography with symmetrical cryptography. 4 The authentication process relies on digital signatures to establish protected communication connections which never need uninterrupted security. 1 2 3 4 Examples & Applications: •Secure email transmissions •Protected web pages •Online financial transactions S ET (Secure Electronic Transaction) The financial institutions Visa and Mastercard together created SET as a solution for protecting online credit card transactions. 1 2 3 This security protocol provided authentication together with encryption alongside message integrity protection but customers failed to adopt it extensively. How It Works: All participants in SET transactions gain identity verification through digital certificates that authenticate cardholders as well as merchants and banks. The encryption technology shields payment details so merchants cannot obtain sensitive cardholder info which decreases fraud possibilities. 1 2 3 36 173 The dual signature

authentication mechanism of this method uses Public Key Infrastructure (PKI) to provide maximum security during transactions. [1][4] Examples & Applications: Secure online payments Credit card transactions for e-commerce (Kizza, 2020)PEM (Privacy-Enhanced Mail) PEM serves as a cryptographic protocol which protects email correspondence through symmetric key encryption and digital signature implementation. [1] PEM provides three essential features in encrypted communications including message confidentiality protection along with integrity defense and authentication capabilities. [1][2][3] PEM depends on asymmetric encryption and hierarchical PKI certificates to ensure message authenticity in communication. Figure 8 PEM Examples & Applications: Secure email communication Digital signature verification How It Works: PEM establishes a dual encryption system of symmetric and asymmetric encryption to establish secure email protection. [2][3][4] The sender starts by applying symmetric encryption to message data before using the recipient's public key encryption for further protection. [4] [100] A signature utilizes digital methods to confirm both the origin of the message sender and authenticates the message content. [4] Examples: Secure email communications in government, military, and corporate environments. This standard encryption solution serves as the main protection system for confidential messages distributed through high-security platforms. (Kizza, 2020)PGP (Pretty Good Privacy) PGP functions as a security protocol which encrypts both email content and file materials along with verifying message validity. The system achieves both security enhancement through symmetric and asymmetric encryption methods. PGP enables message encryption through its system while users can validate their information through digital signatures. [1][2][3] Figure 9 PGP How It Works: The message compression begins before PGP encrypts it by utilizing symmetric encryption algorithms. The symmetric encryption key goes through encryption by the recipient's public key. The sender includes their digital

signature secured by their private key for recipients to verify both message trustworthiness and its original state after decryption. [1] Examples & Applications: Secure email services provide encryption to achieve email confidentiality. Secure file storage functions by applying encryption protection on data sets along with signature authentication protocols. [1] PGP protects both email communication and stored database files through its encryption technology complemented with digital signature verification thus becoming prevalent among privacy-oriented organizations dealing with sensitive data. (Kizza, 2020)PPTP (Point-to-Point Tunneling Protocol) PPTP functions as a VPN protocol which secures data communication across public computer networks. The encapsulation method of Point-to-Point Protocol (PPP) packets happens within a tunnel based on Internet Protocol (IP). [2] [3] PPTP represents one of the most used VPN protocols yet provides less security protection when compared to contemporary protocols. Figure 10 PPTP How It Works: A VPN connection between clients and servers is created by PPTP functionality so both entities can transmit encrypted data. [1] [2] [3] The authentication process relies on PPP standards and Microsoft implements its MPPE (Microsoft Point-to-Point Encryption) optional encryption protocol. The encryption elements of PPTP exist but prove ineffective against contemporary cyber dangers. Examples & Applications: Microsoft VPNs – Used for remote access to corporate networks. Corporate remot e access – Providing basic VPN functionality for remote employees . The PPTP protocol enables secure remote network access but companies seeking superior encryption standards should avoid this method. (Kizza, 2020)Cryptography The cryptographic process of data encoding with algorithms creates data unreadable by unauthorized users through encryption. [1] Secure communication becomes possible because the system protects privacy of data and blocks unauthorized modification. [1] [4] The main cryptographic tools consist of symmetric encryption

along with asymmetric encryption and digital signatures together with hashing. 1 4 31 37 181 Figure 11 Cryptography Symmetric Key Cryptography Symmetric Encryption The encryption process with symmetric methods requires a common key to perform both encryption operations and decryption steps. 1 4 37 Secure transmission between sender and recipient needs identical keys in place. 87 The key distribution issue for large volumes of data constitutes a critical challenge when using symmetric encryption because this method proves highly efficient at data encryption. Figure 12 Symmetric Encryption How It Works: The encryption process uses one single key to turn messages from text into unreadable formats which protects unauthorized users. 1 The recipient employs the very same key provided by the sender to transform encoded information from ciphertext to its original content. 1 Advantages: Faster encryption and decryption due to lower computational complexity. The system effectively handles encryption and decryption of extensive data collections. 1 The implementation process of symmetric encryption proves simpler than what asymmetric encryption requires. Disadvantages: To protect against unauthorized access the method of key distribution must be securely implemented. Any breach of the encryption key exposes every file that remains encrypted. Public key distribution methods make this system incompatible for such applications. 1 Algorithms:Three principal encryption methods used in symmetric algorithms are AES, DES and Blowfish. (Katz, 2020) (Menezes, 1996)Asymmetric Key Cryptography Each asymmetric cryptographic system possesses two separate keys because the encryption process uses a public key whereas the decryption function requires a private key. The encryption system maintains an open accessibility for public keys but preserves total confidentiality for private keys. 1 The increased security of this approach reduces its encryption speed when compared to symmetric encryption techniques. Figure 13 Asymmetric Encryption How It Works: The system generates two related cryptographic keys

consisting of a public component along with a private component. Senders encrypt information using recipient public keys to establish encryption designed for decryption by the matching private keys. [1] [109] Secure key exchange becomes possible through this method because private keys remain undisclosed. Public Key vs Private Key: A semantically secure public-key homomorphic encryption scheme allows conversion into a private-key homomorphic encryption system that requires only slight modification. The encryption key remains available for homomorphic evaluation procedures in public-key solutions but this feature does not exist in private-key implementations. [1] [4] The modification ensures that the private-key system functions as a homomorphic system like the public-key system in both compact and distribution-preserving configurations. Advantages: Security key management becomes easier because users need to protect only their private key. [1] [2] [3] Digital signatures function as strong authentication tools that protects both messages and their communications. [2] [3] The system protects message security regardless of which open networks are used including the internet. [1] [2] [3] Disadvantages: Slower than symmetric encryption due to the complexity of mathematical operations. [2] [3] The encryption of large datasets requires computers with substantial power which impacts performance speeds. Data encryption becomes unfeasible unless the private key is restored after its loss. [1] [2] [3] [4] [7] [9] [11] [12] [13] [17] [18] [22] [24] [25] [28] [32] [37] [39] [41] [42] [49] [53] [59] [73] [74] [78] [94] [130] [174] [184] [186] [187] [190] [191] [207] [227] Algorithm Examples:Three common asymmetric encryption algorithms are RSA (Rivest-Shamir-Adleman) alongside ECC (Elliptic Curve Cryptography) together with Diffie-Hellman. [1] [10] Hashing Hashing functions as a cryptographic process which converts data inputs into static hash values of equal length. [1] Data integrity is maintained through hashing because the method allows users to verify information has not been modified. [1] [12] [41] [74] [181] Hashing functions work irreversibly because the one-way process prevents users from retrieving original data from hash values. [1]

20 Figure 14 Hashing How It Works: The hashing algorithm receives the input for processing then generates an exclusive output of fixed hash size. 1 The unique fixed-length hash value completely changes when the input data experiences even a minimal alteration so hashing functions well to identify unauthorized modifications. The hashing process produces results without the possibility of reverting back to the original information. This means the original data becomes irretrievable. Advantages: The system upholds data integrity because it reveals any modifications. The system computes quickly which enables its use in password storage systems and digital signature verification processes. 4 A hashing operation generates steady output length no matter how large the input becomes. 1 2 3 4 Disadvantages: One-way processing prevents the algorithm from serving as an encryption and decryption solution. A bad algorithm can lead to hash collisions as a result. Brute-force protection against attacks requires the implementation of salting techniques during nominal usage. 1 2 3 4 12 13 17 18 22 24 25 28 36 39 41 43 59 63 72 78 89 125 148 174 176 184 187 191 192 195 231 Algorithm Examples: SHA-256 (Secure Hash Algorithm) and MD5 (Message Digest Algorithm) together with BLAKE2 represent the hashing algorithms most frequently used at present. Digital Signature Digital signatures function as cryptographic authentication tools which verify the authenticity as well as the uncoupled nature of digital material. 185 207 236 Message authentication begins when senders apply their private keys for signature before recipients use their public keys to verify the message authenticity. Both these procedures verify the message remained untampered while ensuring the sender's true identity. 4 Figure 15 Digital Signature How It Works: Message hashing kicks off the process before the private key of the sender is used to encrypt the hash to generate the digital signature. 1 2 3 4 5 7 11 53 60 67 The recipient applies the sender's public key to decrypt the hash after which

they generate a new hash from the received message and perform a comparison. A match between both hash values leads to verification of the message both as unmoderated and originating from the intended sender. 1 2 3 22 133 How It Works: The message hash creation occurs first in the process and then the sender uses their private key to encrypt the hash to produce the digital signature. 1 After decryption using the sender's public key the recipient applies this procedure to the hash and performs a new hash computation of the received message until both outputs match. The matching of hashes between the original and received data reveals the exact authenticity of the information together with its pristine state. Advantages: Because digital signatures verify sender credentials to the recipient. A digital signature protects data integrity because alterations to the message will cause signature invalidation. 2 3 Legal acceptance for secure electronic transactions exists throughout various jurisdictions because of the digital signature standard. Disadvantages: Trust is maintained through the operation of a Certificate Authority but requires their continued operation. 2 3 253 Computationally intensive due to the use of asymmetric encryption. 1 2 3 206 A private key breach will invalidate past as well as future signatures which the sender generated. (Katz, 2020) (Menezes, 1996)Algorithm Examples: The digital signature algorithms known for widespread use include RSA Digital Signature, DSA (Digital Signature Algorithm) along with ECDSA (Elliptic Curve Digital Signature Algorithm). Cybersecurity Standards The cybersecurity standards offer comprehensive guidelines which help protect information systems from potential security attacks and weaknesses. The standards establish guidelines for ideal operational practices that support organizations to manage their risks and safeguard sensitive information alongside regulatory compliance requirements. Through their implementation organizations achieve both cyber threat reduction and essential compliance with various legal

and industrial requirements. ISO 27000 Series Information security management systems receive their worldwide recognition through the globally recognized ISO 27000 standards series. The security standards concentrate on both risk reduction techniques and best practices implementation. 1 The main purpose of ISO 27001 is to manage security controls but specific security-related guidelines stem from other standards found within this series. Organization must develop their security framework continuously and improve it to maintain compliance standards. Figure 16 ISO 27000 SERIES Benefits: International recognition of protected valuable information assets is a benefit achieved through compliance with the standard. The implementation of ISO 27001 guarantees adherence to all legal security requirements and regulations. The organization gains customer trust through its clear security dedication. 1 Impacts: Security breaches together with data leaks become less likely when security measures are implemented. The organization develops operational security capabilities which boost business resilience. 1 4 Raises security expectations for vendors and business partners. (Katz, 2020) (Menezes, 1996)NIST SP 800-53 The U.S. National Institute of Standards and Technology created NIST SP 800-53 as a globally used security and privacy framework that provides comprehensive guidelines. 4 Federal agencies launched this security framework but organizations from both government and commercial sectors now use it for improving their cybersecurity defenses and managing security risks. 1 4 Figure 17 NIST SP 800-53 Benefits: NIST SP 800-53 delivers security controls implementation methods through a systematic process. Organizations can fulfill their FISMA and FedRAMP obligations because of this solution's assistance. 1 15 The framework includes different security areas by educating organizations about risk assessment and incident response planning methods. Impacts: The framework delivers strengthened cybersecurity defense mechanisms which

protect government-operated information systems jointly with private-sector computer platforms. Security weak points decrease while response capabilities improve through the implementation of security measures. 4 Areas of organization governance receive strengthened oversight to enhance regulatory compliance. 1 4 235 NIST SP 800-171 The NIST SP 800-171 framework serves as essential standards which guard Controlled Unclassified Information (CUI) throughout non-federal organizations. 1 4 The cybersecurity framework contains fourteen security domains which are supported by one hundred ten security requirements that stop unauthorized access to sensitive government information. Organizations who work under U.S. government contracts must fulfill the requirements of this standard. Figure 18 NIST SP 800-171 Benefits: The implementation protects official government data which remains in private-sector computing systems. 1 Businesses that process CUI receive an effective security infrastructure through this implementation. Supports all federal regulatory requirements which include the CMMC standards. Impacts: The implementation of this cybersecurity protection system ensures better security for all government contractors. 1 4 The security system strengthens supply chains which support operations with federal agencies. The proper handling of classified information using standard industry protection methodologies occurs through the framework. (Katz, 2020) (Menezes, 1996)NIST Cybersecurity Framework (CSF) The NIST Cybersecurity Framework (CSF) works as an optional and commonly used guide that helps organizations handle their cybersecurity threats through best-practice solutions. 1 4 14 31 127 189 194 222 The framework adopts five core functions – Identify, Protect, Detect, Respond and Recove r – that simplify implementation for organizations ranging from smal l to large enterprises. 1 Figure 19 NIST CSF Benefits: This approach enables organizations to implement risk-based strategies for cybersecurity management which remains flexible. This methodology

maintains security solutions that fulfill regulations and business targets. Managers from both executive leadership and IT achieve better collaboration in risk management through implementation. Impacts: Organizations cut their exposure to risks through enhanced ability to detect and respond to threats. The security solution enhances the speed of response when incidents occur along with the effectiveness of incident management and recovery actions. 1 4 The organization builds up its cybersecurity resistance through the establishment of a strong security culture. (NIST,2018) NIST SP 1800 Series The National Cybersecurity Center of Excellence (NCCoE) produces the NIST SP 1800 series which provides straightforward guidance to handle existing cybersecurity issues. 1 These tested technical solutions found in their publications are specifically designed to address security challenges of individual industries through documented best practices and technology implementation guidelines. Benefits: NIST SP 1800 offers organizations step-by-step guidelines to carry out cybersecurity implementations. Addresses industry-specific security challenges with relevant tools and practices. The documentation promotes organizations to put into practice tested security technologies along with proven methodologies. (OWASP, n.d.) Impacts: The standards improve cybersecurity procedures specifically for healthcare organizations and financial institutions along with manufacturing companies. Real-world effective corporate security solutions emerge through the implementation of the benefits. Organizations can enhance their cyber protection through anti-digital threat solutions which monitor current digital hazard developments. 1 OWASP (2021) Definition: OWASP is an organization that focuses on educating users regarding OWASP Top 10 that is the most important web-related security threats according to a 2021 update. 1 The list focuses on application security vulnerabilities like broken access control problems and injection flaws along with cryptographic

weakness. The OWASP organization helps developers maximize application security using available tools and recommends best practices for secure coding and application security testing. 1 Benefits: Developers and security personnel can find ways to avoid and defend against well-known web security vulnerabilities with the aid of the tool. Offers best practices and open-source tools for secure software development. Security practice and industry standards are encouraged more emphatically while raising overall security awareness. 1 Impacts: Web applications are less vulnerable to security attacks based on OWASP guidelines. 1 Secure coding practices are an essential part of the software development process because of this approach. Companies benefit from security regulation compliance by applying the OWASP framework. MITRE Definition: MITRE works in the public interest as a nonprofit organization that does its work in the creation of security frameworks like ATT&CK (Adversarial Tactics Techniques and Common Knowledge) and CWE (Common Weakness Enumeration). The ATT&CK knowledge base portrays information concerning actual cyber threats but CWE resembles a catalog to be utilized when documenting software vulnerabilities. The security frameworks provide professionals with the tools needed to better understand threats so that they can deal with such cybersecurity issues. Benefits: The organization improves its threat information collection capability through documented descriptions of enemy actions and plans. Security teams are aided by this approach to locate and correct system vulnerabilities. This system offers both people and technology solutions for protecting networks and incident management in an organized way. 1 Impacts: The framework provides improved cyclance detection and response capabilities to cyber vulnerabilities. Defensive structures become stronger because organized security measures are made compatible with concrete attack protocols. 1 Collaboration between cyber security experts and organizations experiences improvement through this process. 1

9 19 35 65 111 112 144 171 175 178 183 185 193 Definition: (MITRE, n.d.) M1 Compare and contrast at least two major Network Security protocols. Introduction The process of Protecting data communication through networks requires network security protocols to establish safe cross-network operations. 28 234 Network security protocols implement encryption together with authentication protocols and data integrity mechanisms to protect networks from unauthorized attacks. 105 121 Currently the most popular type of network security protocols consist of SSL/TLS together with IPsec and SSH. This section delves into the operational characteristics together with security functionalities and application landscapes and operational effects and protection weaknesses of these protocols. (MITRE, n.d.) SSL/TLS The web traffic security protocols SSL and TLS operate as cryptographic systems implemented to protect digital information during transmission. The updated version of SSL called TLS provides better security performance. 91 SSL/TLS functions as a layer-7 protocol to protect network traffic between servers and clients during their communication process. Asymmetric encryption ensures authentication while symmetric encryption ensures data confidentiality through this security protocol. SSL/TLS protocols enable HTTPS secure web connectivity and provide cryptographic encryption together with digital certificate authentication to guarantee data integrity by examining the hash value. Use Cases: Secure web browsing (HTTPS) Online banking transactions Email encryption (SMTPS) Vulnerabilities: The protocol remains vulnerable to POODLE and Heartbleed attacks during its older version operation. 1 Without suitable certificate validation systems vulnerabilities exist for MITM attacks to occur. (MITRE, n.d.) IPsec (Internet Protocol Security) IPsec protects Internet Protocol network traffic by working at the network layer to establish IP security through encryption systems and perform authentication checks and ensure data integrity. VPNs deploy IPsec as their principal security protocol for protecting

networks over the Internet when users access it through unsecured connections. 1 4 55 142 169 IPsec functions in two modes: The Transport Mode protocol encrypts only the information located inside the IP packet. The tunnel mode encryption process covers the entire IP packet therefore offering enhanced protection for transmitted data. 1 2 3 4 13 19 23 32 35 40 47 55 58 61 68 69 73 81 116 154 169 173 179 197 217 The Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols within IPsec components enable the encryption as well as authentication of transmitted data while protecting its integrity. Use Cases: Virtual Private Networks (VPNs) Secure communication between branch offices Site-to-site VPNs Vulnerabilities: The configuration process along with management aspects of this solution prove challenging to administrators. The system remains at risk if properly configured because it faces potential attacks through replay. The heavy dependence on encryption keys makes the system exposed to encryption key breaches when proper security measures for key management are not implemented. (Kent, 2005)SSH (Secure Shell) SSH functions at the application level to enable protected connections for system remote management and protected file transfer operations. 1 2 3 154 174 181 186 187 201 214 223 The authentication and encryption methods of SSH depend on public-key cryptography with common protection algorithms AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman). 1 2 3 22 23 47 71 105 170 171 175 178 204 239 This connection protocol offers remote server control together with secure SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol) protocols. 141 Use Cases: Secure remote login to servers Remote file transfer operations can be conducted through SSH protocols SFTP and SCP. Managing network devices securely Vulnerabilities: The use of weak passwords creates an opportunity for hackers to conduct brute-force attacks. The server becomes exposed to Man-in-the-Middle threats when it skips confirmation of the server fingerprint. 1 2 3 Private keys face the

risk of unauthorized access when they become compromised. (Ylonen, 2006)Comparison of SSL/TLS, IPsec, and SSH Table Summary Security protocols SSL/TLS and IPsec and SSH function at different OSI model layers to secure network communications according to the provided table. SSL/TLS application layer operation secures HTTPS web traffic by encrypting and authenticating identity and securing data. The protocol assists in securing three types of scenarios which include confidential information on banking sites as well as secure e-commerce transactions and defended email communications. 1 37 94 IPsec is a network-layer protocol used to encrypt and authenticate IP packets for privacy protection as well as data integrity. 1 VPN and remote access configuration and site connectivity is the genre of security protocols. 1 2 3 Central secure mechanism for remote access together with encrypted file transfer functions at the application layer with its SSH technology. The protocol provides security for server management alongside encrypted file transfer facilities accessible through SFTP or SCP utilizing public-key authentication methods. Reason for Choosing Specific Protocols The protocols were chosen as they secure network communication at various levels of the protocol successfully. 1 Web browser security and encryption of online financial data need the secure conditions SSL/TLS technology offers for sensitive data. 1 2 3 13 25 49 90 232 Network communications at the layer depend on the IPsec protocol for security since the protocol encrypts VPNs and site-to-site connections and protects remote network access. 1 SSH technology allows the administrators to have remote server management by providing secure access to the administrators to handle servers through encrypted file transfers. (Dierks, 2008) (Kent, 2005) (Ylonen, 2006)Justification for Protocol Selection Different security problems demand particular security solutions for their resolution. 1 Secure information exchange between internet networks relies on SSL/TLS interception protection to develop online security solutions. IPsec

network layer security protects data and provides firm protection for network-hosted communications and remote network access. [1][2][3] The marriage of encrypted server remote management and secure file transfer functionality in SSH protects sensitive operations from unwanted intrusion and data exposure. Difference in Network Security Before and After Using the Protocols Data was transmitted in plain text until security protocols emerged that mitigated information to third-party entities. Networks were exposed to a broad spectrum of threats, such as man-in-the-middle (MITM) attacks, data leakage, and stealing of credentials. Network security is boosted to a top-notch level by the use of these security protocols. [1][2][3] Secure communication is a result of encryption and authentication as well as protection from unauthorized data modification to secure networks from both eavesdropping and MITM attacks. Network communication protection is a result of three security protocols consisting of SSL/TLS, IPsec and SSH that provide data security through authentication while providing reliability which results in more supported network communication. [1][2][3][4] Conclusion Network communications require three essential security measures which include SSL/TLS in addition to IPsec and SSH because they perform separate protective functions. The primary goal of the SSL/TLS protocol is to protect web communication and transactions through its robust encryption system designed for client-server connections. IPsec specializes in VPN and IP network security by delivering strong network-layer encryption along with authentication features. SSH functions best as a secure platform to execute remote system management and file transfers by creating encrypted connections between systems. Protocol systems deliver unique features for particular applications through specific benefits although they possess possible security weaknesses. An organization must select its security protocols after considering

both its security requirements and the nature of protected data transmissions. Full cybersecurity protection depends on correct use and regular update of these security protocols. 1 D1 Evaluate the importance of network security to an organization. Introduction Organizations in the modern interconnected world heavily depend on their network infrastructures to maintain business operations and access data and communicate with other entities. Network security emerges as all-important because sophisticated cyber dangers increase in complexity. Network security effectiveness remains crucial because it protects vital information and supports continuous business operations which in turn preserves organizational trust. The paper assesses why network security matters then details all necessary elements required to develop an effective security system. 1 2. Importance of Network Security Cyber Threat Defense Explanation: The complexity of cyber threats made up of ransomware along with phishing and malware and Distributed Denial of Service (DDoS) attacks have propagated far and wide. Reasoning: Network security solutions provide complete protection against external intruders and data kidnappings and business disruptions within the network. Effect:Enhances immunity to cyberattacks. Security breaches result in minimized financial risks to the organization. 1 The organization establishes trust relationships with customer segments and external community members. 1 CIA Triad (Confidentiality, Integrity, Availability) Assurance The CIA Triad offers an essential framework to protect information by three essential components: • Confidentiality : Explanation: Keeps sensitive information away from unauthorized parties. Reasoning: Data leak protection is based on various techniques such as encryption in combination with authentication controls and access controls. 1 Impact: Promotes privacy and regulatory compliance. 1 Data breaches and identity theft are less possible due to this framework. Integrity: Explanation: Consistency of data

and authenticity is ensured through this method. Reasoning: Hashing mechanisms and digital signatures offer protection from unauthorized data alterations. 1 Impact: Prevents the unauthorized alteration of data. 1 249 Provides users with better service reliability through improved customer experiences. 1 Availability: Explanation: Users can access their network resources via all operating periods due to this network feature. 1 16 Reasoning: Network availability is constant because of redundancy systems in combination with load balancing and DDoS preventing the time events. 1 Impact: Ensure business activities are seamless. This practice offers higher service quality in addition to consistent system performance. 1 242 2.3 Compliance with Regulations Explanation: Every organization must follow data protection regulations like GDPR and HIPAA and PCI-DSS. 1 Reasoning: Adherence to practice of applying industry standards reduces both threats to security and creates confidence between parties and increases security. Effect: Avoids serious fines and penalties. Heightens levels of data protection. More credibility of the organization is built in doing business with customers and other professional partners. 2.4 Financial Stability and Business Continuity Clarification: Business process interruption required together with loss of finance takes place due to cyber attacks. Reasoning: Effective network security use decreases the interruptions in operations and enables quicker recovery of systems. Impact: Decreases loss due to operational downtimes. Imposes disaster recovery procedures. Enables long-term business success. 2.5 Reputation Protection Explanation: A data breach tends to cause irreparable harm to an organization's reputation. Reasoning: Organizations that prioritize security as their top concern are showing responsibility to their stakeholders and customers. 1 2 3 Impact: Builds trust and loyalty with customers. 1 Improves brand image and competitiveness. Organizations that protect their reputation avoid the

loss of customers through negative reputation effects. 1 2 3 110 3. Critical Network Security Components 3.1 Firewalls & Intrusion Detection/ Prevention Systems (IDS/IPS) Description: The system blocks unauthorized access through the use of network traffic filtering and threat detection functionality. 1 Rationale: Firewalls run on predetermined protocols while IDS/IPS systems detect and remove security threats. Effect: Improves network perimeter security. 1 Blocks malware and hacking. 1 Reduces exposure to cyber attacks. 3.2 Encryption Explanation: This encryption process secures data as it moves from and to endpoints and while it remains static. 1 69 Reasoning: Sensitive data that is encrypted is secure because of encryption methods that implement AES and SSL/TLS protocols. 1 Impact: Prevents eavesdropping and data leakage. 1 Secures communication channels. The deployment avoids data breaches through ensuring lawfulness with data protection rules. 1 3.3 Authentication & Access Control Explanation: With this method enterprise systems and their data are only accessible to verified staff. Reasoning: By using three access control methods MFA and RBAC coupled with Zero Trust models companies develop robust access systems. 1 Impact: Reduces risks of unauthorized access. 1 Reduces insider threats. 1 Enhances data protection. 1 3.4 Endpoint Security Explanation: Any user-owned device that is used for corporate network operations will find security an embedded feature of endpoint security. 1 2 3 240 Rationale: Security solutions like Endpoint Detection and Response (EDR) and Mobile Device Management (MDM) safeguard devices from cyber attacks. 1 Impact: Blocks malware at the device level. 1 Utilization of this security feature guards organizations from remote work attacks while also reducing the threats from BYOD policies. The system allows users to have secure means to access company network environments. 3.5 Regular Security Audits & Penetration Testing Explanation: Continuous security monitoring is a vital defense mechanism against modern cyber attacks because they never remain

static. Reasoning: The integration of audit methods with penetration testing allows organizations to discover their weaknesses so that they can implement security improvements immediately. Impact: Enhances overall security defenses. 1 The organization follows all best practices in cybersecurity. 1 Success for the attack becomes less probable because of these measures. 3.6 Security Awareness Training Explanation: Human error is the top reason for cyber incident initiation. Reasoning: Training workers in phishing practices through social engineering and basic cybersecurity practices guarantees organization safety against threat. Impact: Creates security-conscious work culture. 2 3 Carelessness and insider risks are less security concerns for the organization. Strengthens overall organizational resilience. 3.7 Incident Response Plan • Explanation: Security incidents receive swif t and productive reactions through carrying out planned activities. •Reasoning: these plans identify steps to search and retain and investigate and regain activities once there have been cyber-attacks. •Impact: Operational downtime as well as monetar y losses are minimized through proper security measures. 1 Improves coordination in case of security incidents. Improves future security measures. 1 2 3 4. Conclusion Security of business digital assets depends heavily on network security since it helps in adherence to regulation and maintains operations. Security of business against cyber attacks becomes more effective through simultaneous deployment of firewalls together with encryption measures and access controls and endpoint protection and staff training programs. Investment in network security encourages organizations to gain a good business image and obtain customer trust with constant operations in an interconnected digital environment. 1 4 29 30 38 44 171 193 212 P3 Investigate the purpose and requirements of a secure network according to a given scenario. Building a Secure Network Infrastructure The protection of sensitive data needs organizations to establish a security system

from firewalls to encryption techniques and access limitations and continuous data detection technologies. Secure measures provide a defense system which protects sensitive information together with assets from harm. 2 3 Security Planning at Nobel College A structured serious method for network defense stands as an essential requirement for Nobel College to protect critical data and IT infrastructure systems. Protective measures that follow serve as vital components for establishing strong defense systems. a. Next-Generation Firewall (NGFW) A Next-Generation Firewall (NGFW) integrates conventional firewall functions with deeper packet analysis techniques together with application-based filtering systems and protective intrusion capabilities. The tool boosts security protection because it operates at the application layer to control network traffic. Function: The traffic monitoring capability of this system enables it to observe Structures, Users and Data that move across the network. 1 2 3 Active threat defense through the system detects unauthorized access points along with malware as well as data breaches. Security Enhancement: Active threat defense with real-time threat intelligence helps defend against complex cyber threats. The product implements global security protocols by tracking both user activities and application use patterns. Impacts: Reduces the risks of data breaches and unauthorized network intrusions. 2 3 82 113 137 The solution helps businesses maintain compliance with security standards from their industry along with regulations they must follow. 1 2 3 77 132 183 188 189 Intrusion Detection and Prevention System (IDPS) Continuous analysis of network traffic enables an IDPS to detect and stop suspicious activities right when they occur. 2 3 Function: An IDPS operates by detecting security threats while simultaneously taking steps to stop them from occurring. 1 2 3 39 An IDPS integrates signature-based detection with anomaly detection techniques for threat identification purposes. 1 2 3 Security Enhancement: Protects

against zero-day vulnerabilities and advanced cyber-attacks. 2 3 The system enables fast security incident responses which decreases the amount of damage that occurs. Impacts: The device enables administrators to track security threats better and minimizes possible attack exposure. The solution blocks service failures that result from cybersecurity intrusions. c. Virtual Private Network (VPN) Authorized users including students and staff members and faculty members can access the secure encrypted internal network of the college through a VPN. Function: Facilitates secure remote access for users across various locations. Data encryption through VPN protects information from unauthorized entities who seek to access it. Security Enhancement: Safeguards sensitive institutional information from unauthorized access. The VPN provides protected transfer of information when users access networks that are non-trusted or public. 1 Impacts: Provides safe and seamless remote access for users. 1 4 Protects academic research and intellectual property from external threats. d. 1 2 3 4 70 Endpoint Security The security service known as endpoint security safeguards computers along with mobile devices and Internet of Things systems against cyber threats on their endpoints. 1 2 3 4 Function: security systems prevent dozens of harmful elements including malware, ransomware and phishing attempts. 2 3 The network security protocols extend to every device that is connected across the entire system. Security Enhancement: Endpoint security blocks the movement of dangerous software throughout devices that systems administrators have compromised. A system detects emerging threats while monitoring continuously and responds quickly to newly discovered hazards. Impacts: Security risks from unmanaged personal devices are prevented due to this measure. 2 3 Strengthens the overall cybersecurity resilience of Nobel College. 1 2 3 Nobel College can strengthen its cyber defense and protect its sensitive data through the implementation of these essential security measures to

maintain continuous educational research operations. e. Security Information and Event Management (SIEM) Definition SIEM solutions aggregate and analyze security data to detect, investigate, and respond to cyber threats in real-time. Function: Centralizes security event management across the entire network. 1 Uses AI-driven anomaly detection to identify potential threats. 1 Security Enhancement: Offers instant access to security incidents, enabling faster response times. 1 4 Provides forensic analysis capabilities for detailed security investigations. Impacts: Enhances visibility into network security trends and potential risks. 1 4 16 34 Simplifies regulatory compliance and audit reporting, ensuring adherence to industry standards. g. Network Access Control (NAC) Definition: NAC enforces security policies for devices attempting to access the network, ensuring only authorized users and compliant devices are allowed entry. 1 Function: Verifies device compliance with security standards before granting network access. Restricts access for non-compliant or unauthorized devices to maintain network security. Security Enhancement: Blocks unauthorized access to critical resources, minimizing exposure to threats. 1 2 3 4 Strengthens authentication measures through multi-factor verification, ensuring only legitimate access. Impacts: Shields the network from both internal and external security threats. Prevents malware infections from untrusted or non-compliant devices. By implementing these advanced security measures, Nobel College can establish a robust and resilient IT infrastructure, better equipped to address the evolving cybersecurity challenges faced by educational institutions. 1 2. Purpose of a Secured Network A secured network ensures the protection and integrity of the data and systems within Nobel College, with the following key objectives: Protection of Sensitive Data: Ensuring that student records, research data, and financial information are encrypted and access-controlled to prevent unauthorized access. Prevention of Unauthorized Access: Implementing strong

authentication mechanisms to limit access to authorized personnel only, ensuring that sensitive systems are secure. 1 Network Integrity and Availability: Preventing cyber-attacks and disruptions that could affect educational services, online platforms, and research activities. 1 Compliance with Legal and Ethical Standards: Adhering to data protection laws, including GDPR and HIPAA, to avoid penalties and ensure privacy standards are met. Mitigation of Cyber Threats: Deploying preventive security measures, such as firewalls and intrusion prevention systems, to protect against cyber threats like ransomware, phishing, and malware. 1 Secure Collaboration and Communication: 1 Safeguarding communication channels and collaborative tools used by students, faculty, and staff, ensuring privacy and data protection. 1 3. Things to be Protected Nobel College must focus on securing several critical assets, including: Student and Staff Records: Protecting personal and academic data from unauthorized access or tampering. 7 11 42 53 99 140 Research and Intellectual Property: Safeguarding academic research and intellectual property to prevent theft or unauthorized use. Learning Management Systems (LMS): Ensuring platforms like Moodle or Blackboard are protected from hacking or malicious activities. Wi-Fi and Network Infrastructure: Encrypting both wired and wireless networks to prevent unauthorized access and monitoring for vulnerabilities. 1 Email Communication: Preventing phishing, spam, and email spoofing by using proper email security protocols and filters. 1 Cloud and Storage Systems: Ensuring regular backups, encryption, and access control to prevent data loss or unauthorized access to cloud-based services. 4 Physical Security of IT Assets: Ensuring physical protection of servers, network equipment, and data storage devices from theft or damage. 1 Administrative Systems: Protecting financial, HR, and administrative systems from fraud, theft, and unauthorized access. Conclusion A thorough network security plan at Nobel College will boost protection of sensitive data and enable regulatory compliance while

ensuring both student and staff safety in their environment. The institution's digital operations stay supported with this strong approach while it reduces cyber threat risks. (Cole, 2011)P4 Determine which network hardware and software to use in this network. Network Hardware A network consists of physical hardware components which maintain data communications and transfer operations between networked devices. 1 A secure and efficient data movement operates through switches routers firewalls access points and servers which perform together as complete units. 1. Switches Definition: The device known as a switch serves two functions including network device connection and data packet routing to their correct delivery destinations. 1 2 3 4 98 139 156 160 196 213 243 Switches function at Layer 2 (Data Link Layer) in the OSI model to reach their purpose by using MAC addresses for operation. 2 3 Figure 20Switch Purpose: Network efficiency relies on switches since these devices minimize congestion and improve device communication and help build scalable well-organized network infrastructure structures. 1 2 3 4 Recommendation: Users should use managed switches for bigger network deployments yet smaller home or small office networks need unmanaged switches. Examples: Cisco Catalyst 2960 TP-Link TL-SG108 Netgear GS308 2. 4 12 17 41 Multilayer Switch Definition: A multilayer switch performs Data Link (Layer 2) and Network (Layer 3) functions of the OSI model while integrating attributes from switch and router systems. These devices find practical use in extensive networks to achieve enhanced efficiency and lower network delay. 1 Figure 21 Multilayer Switch Purpose: These switches serve two objectives by optimizing network segmentation for VLANs and inter-VLAN routing to provide quick traffic management capabilities while reducing the need for routers in internal communication. Recommendation: These devices should be used by organizations that need to process data quickly and maintain efficient network traffic flow within their enterprise systems. 1 2 3 4 Examples: Cisco

Catalyst 3850 HP Aruba 2930F Juniper EX3400 3. Router Definition: Network devices operate as routers because these devices link different networks and transport data packets between them based on IP address information. [1][117][121][215][251] These devices function at the Network Layer of the OSI model along with Layer 3. [1] Figure 22 Router Purpose: The primary function of routers consists of internet connectivity management through firewalls and VPNs and traffic control between networks. [1][4] Network segmentation benefits from routers which enhance security performance at the same time. The recommendation states that enterprise-level networks must deploy routers with enhanced security features as simple routers fulfill basic requirements for home or small office applications. [1][2][3][4] Examples: Cisco ISR 4000 Series TP-Link Archer AX6000 MikroTik CCR1036 4. Firewall Definition: The purpose of firewalls is to deliver network traffic governance through rule-based protocols which ensure protection against unauthorized entry and protect the network from cyber threats and malware intrusion. Figure 23 Firewall Purpose: Firewalls serve to block dangerous network traffic while enforcing security regulations through hardware components or software systems or unified hardware-software systems. [9][27][122][173][188][224] Next-Generation Firewalls (NGFW) should be recommended for enterprise networking environments because they enable advanced packet inspection alongside intrusion prevention capabilities. [1][2][3][4][14] [15][26][33][102][219] Examples: Fortinet FortiGate 60F Palo Alto Networks PA-220 Cisco ASA 5506-X 5. [154] Access Points Definition: The Wi-Fi extension system consists of Access Points (APs) which function as network connectors for wireless connectivity throughout network coverage. These devices prove invaluable when wired cabling solutions do not cover extended spaces. [2][3] Purpose: APs serve two key functions through their enhancement of wireless coverage and their ability to enable simultaneous device connections thereby meeting the Wi-Fi requirements of businesses and campus areas and public domains. [1][2][3]

Recommendation: Enterprise-level access points with Wi-Fi 6 support should be used to achieve high-performance network connectivity. [1][2][3][4] Examples: Ubiquiti UniFi UAP-AC-PRO Cisco Aironet 1815i TP-Link Omada EAP245 6. Servers Definition: Powerful systems called servers make network-connected client devices able to access data resources and services. The system controls all operations associated with storing and processing network applications and handling files. [2][3] Figure 24 Server Purpose: Business processing becomes more efficient because servers function as centralized data storage facilities while hosting applications for managing diverse network operations. Thus servers enable both increased scalability and improved security standards for businesses. Recommendation: Business type should determine server selection since large enterprises need high-performance servers over smaller businesses that require mid-range servers. [1][2][3][4] Examples: Dell PowerEdge R740 HP ProLiant DL380 Network Software Network software consists of applications with tools that help manage both network security and communication along with administration of network infrastructure. [1][2][3] Network performance setup through configuration alongside monitoring and optimization tasks helps achieve secure dependable operation of network infrastructure. [1][2][3][4][50][202] 1. Network Operating System (NOS) The Network Operating System (NOS) functions as a critical system to control network resources while connecting devices the network manages. [1] This system delivers services which cover file sharing platform and user administration tools together with security framework capabilities. Purpose: The main functions of NOS include centralized network administration combined with resource distribution features together with access control systems and authentication capabilities. Recommendation: Organizations should select a Network Operating System that corresponds with their network systems and demonstrates capacity to scale according to their needs. [1][2][3][4] Examples: Windows

Server 2022 Linux (Ubuntu Server, CentOS) Cisco IOS 2. Network Configuration and Management Software Administerors can use this software to monitor and configure network devices in addition to performance optimization through automation tools and real-time monitoring features and troubleshooting functions. Purpose: This software serves a dual function that boosts network performance through automated configuration deployment and helps protect security through misconfigurations and vulnerability detection. 1 Recommendation: It is recommended to choose software that incorporates features of automation along with scalability and real-time analytics to achieve better management solutions. 1 2 3 4 6 40 61 63 106 145 195 248 Examples: SolarWinds Network Configuration Manager Cisco Prime Infrastructure PRTG Network Monitor 3. 1 2 3 4 Network Security Software Network security software defends networks against cyber threats through protection of unauthorized access and malicious malware as well as stopping data breaches. The security system should incorporate antivirus tools together with IDS devices as well as endpoint protection software. 1 2 3 Purpose: Network security software serves dual purposes which include protecting data through three main pillars of confidentiality and integrity and availability while helping organizations follow security regulations. 1 2 3 4 Recommendation: Use a combination of firewall, intrusion prevention, and endpoint security solutions for comprehensive protection. Examples: Fortinet FortiClient Palo Alto Cortex XDR Symantec Endpoint Security 4. 1 4 Networking Protocol Software The networking protocol software establishes device-to-device communication through standardized rules such as TCP/IP DNS and DHCP to achieve efficient network data exchange. Purpose: Networking protocol software functions to establish reliable device-to-device communication and controls IP addresses together with routing protocols and domain name resolution. Recommendation: Organizations should choose their networking protocol software

following network requirements while also ensuring compatibility with their present infrastructure. [1][2][3][4] Examples: Cisco IOS (for routing protocols) Windows DHCP Server BIND (for DNS) 5. [1][4] Cloud Networking and Virtualization Software The software solution enables businesses to handle and implement their network infrastructure through cloud platforms. [1] This software operates VNF technology alongside SDN capabilities. Purpose: Network components virtualization through this solution enables flexible cloud-based services that deliver scalable efficiency along with reduced costs without requiring physical hardware. [4] Recommendation: Select a solution which works smoothly with cloud systems and features automated capabilities. [1][2][3][4] Examples: VMware NSX Microsoft Azure Virtual Network AWS Virtual Private Cloud (VPC) 6. [4] Network Communication Software Explanation: The application enables communication through sharing messages and video calls with file exchanging features over network connections to support real-time teamwork. [1] Purpose: The solution achieves higher teamwork performance through dependable communication methods to boost productivity. The system provides high value to organizations that need protected and efficient team collaboration especially through remote operations. Recommendation: Choose new software that combines security features with scalability capabilities alongside ease of integration with existing tools. [1] Examples: Microsoft Teams Zoom Slack (Wireshark Foundation, 2024) How Hardware and Software Work Together to Improve Network Security Different hardware elements together with computer software systems create multiple defensive layers which protect networks from cyber-attacks. [1][2][3] Network security improvements result from physical defense systems and traffic management functions provided by hardware devices including firewalls with IDPS and HSMs and NAC devices. Security keys maintained by HSMs defend encryption protocols used in secure network operations whereas firewalls defend against unauthorized access attempts.

Hardware solutions collaborate with software platforms that include firewalls, antivirus tools, encryption programs, VPNs as well as SIEM systems. 1 The administration of security traffic employs firewalls as filters of dangerous data while antivirus solutions cleanse malware systems and SIEM solutions analyze security records to detect suspicious system activity. Multiple access control software features that integrate biometric recognition systems and multi-factor authorization protocols stop unauthorized users from entering the system. Both hardware elements and software form a comprehensive security defense mechanism. HSMs function as secure locations for encryption keys while encryption programs maintain information confidentiality. The combination of firewalls stops attacks at the same time software updates eliminate system vulnerabilities. Network security builds its strength by harnessing computer system hardware to physically protect operations and software-based intelligence to detect threats thus minimizing potential risks and cyberattack vulnerability. 1 9 19 30 35 38 112 171 175 178 183 185 193 M2 Create a design of a secure network according to a given scenario. 1 Figure 25 : Initial Design of the Network Network Design of Nobel College The network design at Nobel College unites different components which operate as a single unit to deliver safe and efficient connection throughout the institution. The network components including routers and firewalls as well as switches and servers and end-user devices maintain a hierarchical pattern which allows secure and smooth data transfer throughout the network. 4 Key Components in the Network 1. 1 4 5 Router The 2911 Router operates as a communication gateway between internal networks and external networks which include the internet. The network system handles data flow by controlling the movement of packets while performing routing functions correctly. The router serves as a gateway to direct data packets between the internal network and external networks since it manages proper routing of

data between both domains. The device has an essential function to control network traffic and make internet connectivity possible. 2. Physical Firewall The Cisco ASA Firewalls act as protection systems which conduct traffic inspections to stop unapproved network access. Such hardware blocks external security threats by sitting in between the network router and the internal area. The firewall serves to detect all network traffic movement according to defined security rules through which it blocks unwanted traffic to safeguard internal network integrity. Such systems act as the main shield against harmful cyber disruption. 1 3. Multilayer Switch The core part of the network features a multilayer switch which performs Layer 2 switching along with Layer 3 routing functions. The device supports fast data exchange operations and controls network traffic between access switches and servers and the firewalls. This network core element functions as the main management unit that controls traffic movement between access points and servers while protecting the firewall through its purpose. This device enables smooth data exchange between diverse network areas through its central role in controlling internal data movement. 1 4. Access Layer Switches (3) Three Cisco 2960-24TT switches operate at the access layer to connect PCs and servers as well as other end-user devices to the network. The internal network functions with help from these switches which manage data transfer between devices. The access switches function to deliver network access to devices which they forward through the core multilayer switch. Through these switches user devices and servers obtain their main access to all available network resources. 4 5. Servers (4) The network contains four servers which perform duties as application hosting units and data storage facilities together with network services administration functions. The servers connect to access layer switches to exchange information with other devices

present in the network. 98 The servers deliver essential resources which include file storage functionality as well as web hosting features and network administration capabilities. The institution depends on these servers to maintain its IT infrastructure and deliver functional services to end users. 1 6. End-User PCs (6) End users gain access to network resources through six PCs whose connections lead to the access switches. Users (including students and faculty along with staff members) access network resources to perform tasks like internet browsing while using applications through their PCs enabled by the PCs. 1 Limitations of the Current Network Design The whole network goes down as soon as the router is down. The network only employs static routing when this method becomes expensive and inefficient for growth and development-based networks. 1 The network is secured by a single firewall without employing Additional Security features such as Access Control Lists (ACLs). 1 The whole network is in one domain without a VLAN system leading to congestion and increased security threats. The network lacks traffic management capability since it does not apply load distribution methods that would otherwise enhance speed of performance. Cloud services and scalability operations in addition to backup operations are not supported by this network. Network Summary The network implements a hierarchical structure starting from a router at the top equipped with firewall security. The core multilayer switch functions as the key element which controls the traffic flow between access switches and servers and end-user devices. The network traffic remains inside each zone through access switches whereas servers serve as vital resource suppliers and distributers. The Cisco ASA Firewall functions as an authorized entry point by protecting the network from unauthorized traffic as it operates as a gatekeeper between external and internal systems. The implementation of

multilayer switches combined with access switches results in rapid data transfer which reduces network delays along with maintaining high levels of system efficiency. 42 182 This network design ensures the efficient and secure operation of Nobel College's IT infrastructure, facilitating smooth data flow and providing reliable access to network resources for students, faculty, and staff. 1 Enhanced Network Design The improved network design utilizes cutting-edge technologies to improve security, reliability, and performance. Upgrades include HSRP, OSPF, VLAN isolation, ACLs, and cloud computing services. Key Improvements: Key Enhancement: Improved Firewall with More Security: It provides strong traffic filtering along with better protection policies and complete record-keeping functionalities. 1 28 Implemented policies enable the system to control all incoming and outgoing traffic from and to the network boundary. 1 15 21 45 176 HSRP (Hot Standby Router Protocol): The system provides backup router functionality to automatically replace the failed primary router. 1 The system reduces downtime intervals by its operations which provide uninterrupted network connectivity. 1 2 3 26 OSPF (Open Shortest Path First) Dynamic Routing: Dynamic Routing offers automatic route calculation as well as network topology adjustment via changes. 1 The routing system provides automatic route calculation which changes when network changes occur. The system provides better performance by ensuring optimal network traffic flow. Inter-VLAN Routing: The network is divided by VLANs for security functionality and traffic optimization capabilities. An isolated network segment is enabled for different business groups to work on their own. Access Control Lists (ACLs): Security enforcement of traffic is achieved through the allowance or denial of certain kinds of traffic. Security policy as well as prevention of authorized access is included in this system. 1 2 3 5 Cloud Integration: Cloud services have to be employed to achieve performance enhancements

and scalability benefits. The use of backup and disaster recovery solutions through technology reduces infrastructure costs. Comparison Table: Current vs. Enhanced Network Design Justification for Using Multiple Devices Redundancy: Service delivery remains uninterrupted if a device fails. 1 Load Balancing: The system distributes traffic load evenly to prevent system slowing. Security: Offers extra layers of security via firewalls, ACLs, and VLANs. 1 5 Scalability: Accommodates future expansion without major changes in configuration. Conclusion The existing setup is functional but missing key features for redundancy and dynamic routing capability and cloud support. The design enhancement melds improved security with higher uptime and performance via the utilization of HSRP and OSPF and inter-VLAN routing and ACLs and cloud services. 1 The network enhancements enhance traffic performance and reduce equipment downtime and create a system capable of scaling based on future business growth needs. 1 4 P5 and M3: Network Design Explanation Figure 26 Secure Network Design for Nobel College A design of Noble College's network was built with Cisco Packet Tracer and it can be observed in the Secure Network Design for Nobel College figure. Packet Tracer provides users with an effective platform to test and simulate virtual network designs. 1 Each department follows a simple color scheme: servers use pink, students employ red and teachers use red and heads use yellow for identification. The networking devices link up all departments within this system. Designers arranged network devices systematically to establish protection protocols alongside backup systems in the entire network. The network receives fundamental protection from outside threats because the firewalls that connect to routers serve as a front line defense system but server protection increases through additional firewalls placed near the server room. 1 4 The departments remain connected to internet access yet they maintain internal network communications since all departments remain

within the organization's internal systems. Security across the network depends entirely on ASA firewalls to ensure protection of the network system. Devices and Configuration Overview Switches: The design system features four Cisco access layer switches as its fundamental component. Why Use Switches? Every business needs switches to maintain high-performance network connections between their departmental groups. The devices operate only to deliver data to proper destinations thus preventing network congestion along with improving system performance. 237 The network security is improved through VLAN implementation enabled by switches that create separate zones to isolate traffic thus controlling unauthorized access. VLAN Configuration Why VLANs? 8 45 This network design uses VLANs because these logical divisions of LANs enhance performance above physical separation. 1 45 VLANs enable organizations to reduce broadcast traffic flow and secure their sensitive data while providing easier network administration. 45 System modifications become possible through VLANs which do not demand physical infrastructure changes. Network configurations face regular changes which become easier to handle because VLANs offer flexibility. 1 Justification: The formation of VLANs enables networks to secure operations by regulating the separation of traffic between segments for the purposes of gaining increased broadcast domain reduction and performance. Greater operational framework and simpler management of networks are accomplished with VLANs. VLANs lead to data segmentation to protect network data transfer. Network scalability is achieved in VLAN-based networks because growth operations possess identical degrees of security alongside identical performance behaviors and management functions. 1 4 5 Configuration: For Students: For Teachers For Head Department For Servers Multilayer Switch In this configuration, four multilayer switches are used to enhance both performance and functionality Why Use Multilayer Switches? Multilayer switches hold great importance because their dual functions as

Layer 2 switching devices and Layer 3 routers enable critical network services. [1] [2] [3] [4] [64] The key functions for Multilayer switches also support DHCP pools and Inter-VLAN routing alongside HSRP (Hot Standby Router Protocol) and OSPF (Open Shortest Path First) and ACLs (Access Control Lists). [1] The switches perform DHCP functionality because it guarantees the dynamic distribution of internet protocol addresses. The feature provides critical features for departments to transmit data through secured VLAN routes. The network hardware facilitates deployment for dynamic routing by OSPF and high availability by HSRP as well as security enforcement by ACLs. Configuring Inter-VLAN Routing Inter-VLAN routing is enabled by the network administrator to enable communication among different VLANs in the network system where security and identity of each VLAN are not compromised. Routing setup enables security stability and speed of operations through enabling VLAN traffic to move across network segments at high speeds. The configuration used enables the network to support effective communication among departments that translates into better performance and protection of the network system. [1] Justification: Through Inter-VLAN routing network devices within isolated virtual local area networks can communicate with each other. [1] The network security is improved with traffic isolation and domain broadcast reduction as effective data route distribution is still maintained. [1] Layer 3 switches and routers used through Inter-VLAN routing integrate networks without slowing down operations. [1] [2] [3] [4] [5] [12] [17] [64] Verification: Configuring DHCP Reasoning:A network setup with DHCP automates configuration processes to distribute IP addresses and subnet masks and other network parameters to devices automatically. The centralized operation shortens administrative work while lowering configuration errors thus optimizing resource allocation especially in extensive or evolving network structures. [1] [2] [3] [8] [20] [36] [48] [51] [56] [57] [75] [84] [88] [100] [103] [119] [136] [150] [196] [208] [213] [215] [241] Justification: Network appliances

automatically receive IP addresses from DHCP acting as the Dynamic Host Configuration Protocol server. 1 2 3 8 12 17 46 51 57 79 88 129 150 153 230 Network address assignment, subnet mask assignment, default gateway and DNS server data distribution happen automatically without any manual intervention by using DHCP. Efficient network management is provided by the system with removal of human-intervention-related errors. Verification: Configuring HSRPReasoning: A total network breakdown becomes avoidable through HSRP's operation. The system verifies router availability through its standby mechanism which selects an active router responsibility backed by a standby device. 1 Fine network transitions happen after active router outages because this configuration enables continuous device connectivity. 1 2 3 6 21 80 152 176 Justification: Cisco Hot Standby Router Protocol (HSRP) is a protocol for redundancy that is system-specific and provides constant availability of network gateway routes. 1 The protocol allows routers to cooperate by offering a single virtual gateway IP address to the network. failed primary routers are replaced by standby routers that take over control to reduce network downtime. Verification: This implementation design positions the multi-layer switch as the active router component. The standby router functionality exists in Multi-Layered Switch 2. Configuring OSPFReasoning: The transmission process in OSPF functions dynamically to improve network routing and packet forwarding. The protocol selects optimal data paths through networks while it responds instantly to current network changes. 1 OSPF functions as a link-state protocol which enables it to deploy quick responses to network topology changes while choosing optimal routes for improved scalability and reliability and better performance. 1 2 3 5 6 10 169 170 179 180 198 200 208 225 Justification: Open Shortest Path First (OSPF) is a link-state Internet Protocol (IP) network routing protocol employed to implement dynamic implementations of data routing. 1 2 3 OSPF technology

shares the routing information of routers in an equivalent autonomous system through the performance of Dijkstra's algorithm used for shortest path calculation. OSPF operates in such a manner as to utilize rapid convergence along with best routes. 1 2 3 5 6 10 169 170 179 180 198 Verification Configuring ACL configuration: Reasoning: OSPF (Open Shortest Path First) is an IP network link-state routing protocol utilized in the implementation of dynamic data routing. 1 2 3 OSPF shares routing data between routers of the same autonomous system based on Dijkstra's algorithm for computing shortest paths. OSPF operates through the delivery of quick convergence and best path routing features. 1 Proper configuration of Access Control Lists (ACLs) is required as the foundation for network security since they enforce predefined rules to govern network traffic access. ACLs help create security policy and block unwanted traffic while filtering for compliance and subnetting network segments and keeping valuable resources safe and providing incident tracking because they can record network activity and observe traffic behavior. Justification Network security deeply depends on accurate Access Control List (ACL) setup as ACL is a control mechanism for granting network traffic access based on a pre-set approval policy. ACLs are functionally similar to security enforcers and provide protection while avoiding unnecessary waiting traffic, maintaining control and ensuring observation by monitoring over compliance as well as providing isolations mechanisms and protect important assets by monitoring communications backtraces alongside activity records. Verification The efficiency of ACLs is validated by observing network traffic, reviewing access logs, and ensuring that only authorized users and devices have communication privileges while blocking unauthorized access attempts. Security DevicesWhy Use Security Devices? The Adaptive Security Appliance (ASA) is employed to secure the network by blocking

unauthorized access, potential threats, and intrusions. It acts as a firewall between the internal network and the internet and provides stateful packet inspection, VPN (Virtual Private Network) support, and intrusion prevention, making the network secure and safe for Noble College. Reasoning: Installing a firewall is crucial to network security, as it controls traffic and protects against potential attacks. It enforces security policies, enhances network performance, and protects sensitive resources from cyber-attacks. A well-configured firewall prevents unauthorized access, enhances network stability, and enhances resilience, hence ensuring better performance and reliability. 1 2 3 4 Verification Router: Why Use a Router? The router serves the important function of linking Noble College's internal network with the external network and the internet. 1 By routing data between different networks, it enables easy communication between local devices and external services. 244 In this setup, the router is used as the gateway, allowing internet access and communication with the outside world. It also optimizes data transmission by selecting the best routes, thus ensuring efficient utilization of network resources and high-speed connectivity. 1 2 3 4 5 6 10 16 26 44 62 77 169 170 179 180 200 203 Function of OSPF in Router Configuration: Open Shortest Path First (OSPF) is a dynamic routing protocol that automatizes the distribution of routing information between routers. OSPF provides dynamic routing for this network topology by adapting to changes in topology, making sure that data is forwarded via the most preferred paths. 170 OSPF operates by distributing routing information and determining route costs, allowing the router to determine the shortest and most efficient data paths. This minimizes latency, enhances reliability, and offers dynamic rerouting in case of network failures. The role of the router in OSPF configuration ensures timely routing decisions, fostering scalability, flexibility, and stability. 1 As network requirements grow, OSPF

dynamically adjusts to maintain optimal performance, allowing the Noble College network to accommodate growing traffic and the addition of new devices efficiently. Nodes: Laptops are utilized for wireless connectivity, while PCs and servers rely on wired connections for stable and high-speed data transmission. 1 4 6 PCs:A total of 12 PCs are included in this network setup, all connected via Ethernet cables to switches, ensuring a reliable and efficient wired connection. 1 Laptops:A total of three laptops are integrated into the network, utilizing Access Point (AP) services to establish a seamless wireless connection. 1 4 6 Servers: Total of 4 servers(file,dhcp,dns and database server) are used in this network. Configuring the Servers. 1 2 4 6 8 30 46 50 76 79 80 83 84 92 124 180 199 202 205 229 DNS configuration: Reasoning:An individual DNS (Domain Name System) server converts domain names into corresponding IP addresses that can be interpreted by network equipment. 1 3 4 6 46 51 83 171 175 178 205 When users enter the name of a website in the browser, the DNS server communicates it to the corresponding IP address, ensuring easier access to web resources. It relieves users from remembering numerical IP addresses, performing a function closer to that of an electronic directory that ensures easy travel to the intended online destination. 5 54 Verification Print ServerReasoning: A print server, which can be hardware or software, allows different users to access and share printers on the network. 8 21 48 A print server centralizes the administration of the print tasks so that printers can manage their configurations, queue the prints, and maintain a record of the printing process. The centralized approach keeps the printers consistent and efficient and makes the printing process on the network well-organized and error-free. 76 Verification: File ServerReasoning: A file server is a system or machine that holds and shares data, such as documents, pictures, and videos, with other machines on the network. It is a central source, allowing

users within the same network to access, retrieve, and edit common files with ease. Centralization simplifies file management and facilitates collaboration among network users. 5 54 Configuration Verification Database Server: Reasoning: A database server is an expert system or software employed to store, manage, and make databases available on the network. It's responsible for arranging, querying, and processing large amounts of data optimally in a way that makes it accessible for concurrent use by various users or applications. They are responsible for handling data, improving decision-making processes, and facilitating the proper execution of business operations through the provision of real-time data analysis and retrieval. Why use cloud?Reasoning: The addition of cloud to the Cisco Packet Tracer network architecture provides central storage of data and processing power. Cloud services are economically scalable and flexible as they spread resources over the internet, maintaining the network efficient, scalable, and dependable. Cloud services minimize the need for physical infrastructure, making it possible to manage resources better and access resources anywhere at any time, enabling companies to achieve more in their operations. 1 2 3 Key impacts of using Cloud Cloud deployment within networks utilizes a traditional system reliant on on-premise infrastructure whose set-up demands heavy hardware investment and running costs alongside personnel charges. Scalability may have restrictions that force organizations to acquire additional physical assets they cannot make full use of or that are difficult to scale according to changing demands. This kind of deployment incurs high levels of costs and inefficient resource management methods. Security for data protection and backup creation as well as deployment of disaster recovery necessitates huge resources involving dedicated hardware and expert staff. Companies obtain enhanced scalability functionality from the use of

clouds because they are able to quickly modify their amounts of resources in response to current requirements thus gaining lower expenses together with improved system performance. 1 2 3 Firms that adopt the cloud have operating expenses instead of capital expenses because they only need to buy what they consume. Cloud technology adoption offers employee-level flexibility that allows people to access resources anywhere thus improving remote work capabilities and supporting global collaboration. 1 2 3 228 Cloud infrastructure services strengthen companies by offering dependable backup support and duplicated systems as well as disaster recovery systems that minimize downtime risks. 1 2 3 Security measures include sophisticated encryption methods in addition to access control security as well as industry standards compliance to protect data as well as regulatory compliance. 1 16 199 Quality of Service (QoS): Planning the network with Quality of Service (QoS) allows administrators to prioritize and organize network traffic for the delivery of consistent application performance. 1 2 3 Network configuration that operates with QoS guarantees essential applications like video calls and streaming and file transfers their required bandwidth and prevents delays and congestion. 1 Scenarios with high network traffic coupled with low bandwidth need the deployment of QoS to function optimally. ii. Prioritization of Security-Related Traffic and its Significance in Network Security: The selection of network traffic that is security-centered constitutes fundamental aspects in the modern information security framework. Network security information such as intrusion detection/prevention system traffic and firewall traffic needs to be prioritized over other forms of transmission through the prioritization tool. QoS value prioritization is utilized by the system for enhancing security protocols and applications within the network. Significance in Network Security: Prompt Threat Detection: Security devices can't

afford latency since this enables them to detect threats such as DDoS attacks and malware and unauthorized access. Secured security traffic flow isn't interrupted by lower-priority network traffic flow in these systems. Avoiding Traffic Bottlenecks: Security traffic, when not accorded proper priority, suffers delayed delivery which not only slows down security system responses but also leaves the network vulnerable to attack. Preserving Data Integrity: Security patches are more efficient because networks maintain their integrity as they give priority to time-sensitive traffic. iii. Predictable and Reliable Service: Traffic that is received from the network is predictable because it experiences minimal delay and packet drop or jitter variation when the network is at peak usage. Networks that implement QoS maintain operational effectiveness while processing enormous amounts of traffic to ensure that vital services are not disrupted. [1][2][3] How QoS ensures reliability and predictability: Traffic Policing and Shaping: QoS utilizes Traffic Policing and Shaping to specify transmission rates for data to avert congestion thus ensuring reliability of service. Low Latency for Critical Applications: Quality of Service can serve applications that require low delays so packets are given priority to less important network data which improves performance as well as delivery speed. Traffic Classification and Marking: QoS Traffic Classification and Marking selects traffic types such as voice or video or web traffic to optimize essential service bandwidth usage. The implementation of QoS provides organizations with a tool to maintain reliable high-quality network performance that ensures uninterrupted operations of vital network services. [1][2][3][5] Syslog System administrators utilize Syslog protocol as their default means of gathering and storing log messages from network devices and servers as well as applications. Centralized logging is made possible by this protocol

to enable administrators to deal with system problems more efficiently. The protocol classifies messages by severity based on an emergency rating at level 0 and debugging messages are given the value level The message classification scheme used shows the severity levels of arriving messages. [1][2][3] Timestamped log messages in syslog allow you to track devices while you track message types with event descriptions for enhanced system problem identification and suspected action determination. A syslog network contains a syslog client that sends log files and a syslog server as the log repository facility. The server retrieves log messages through its UDP or TCP connection from devices it has set up. [1] Network management is supported by Syslog by enabling the ability to make security monitoring as well as system structure and compliance requirements possible. [1] Prevention as well as protocol requirements become possible because of syslog, which maintains organizational readiness against possible threats. (Systems, 2023) (Zhang, 2021) (Schmidt, 2020)P6: Comprehensively test your network using the devised Test Plan. [1][5] 1. Introduction to the Test Plan and Its Importance Test plan defines the principal document that summarizes the strategies and methods needed to test network security implementations. [1] The document serves as a blueprint for proper implementation and proper functioning of firewalls and VLANs and ACLs in accordance with design requirements. A test plan delivers a systematic network security testing methodology so that operators can thoroughly test for security threats and guarantee control systems and network protection against malfunctions and cyber attacks. [1] Importance of the Test Plan Weakness Identification: The security audit tool is an identification system to locate security weaknesses in network technical designs. Security Control Validation: The process confirms correct operation of security controls by checking active mechanisms which include firewalls and VLANs and ACLs. Network

Resilience: Network resilience strength assessment ensures that it determines how secure the network is when attacked and system failure. Verifies Security Requirements: Security requirements verification occurs to validate implementation of protective measures that ensure the network is secured against unauthorized access. [1][2][3][5] 2. Identification Objectives The primary objectives of the test plan are: VLANs, Firewalls, ACLs, HSRP, and OSPF Verification: The test verifies VLANs together with Firewalls and ACLs and HSRP and OSPF proper implementation. [1] Enforcement of the Security Policy: The security policy enforcement tests to verify correct implementation of traffic control and resource segmentation policies and access control rules. Redundancy Testing: The test will analyze the effectiveness of HSRP and other redundancy mechanisms with redundancy testing tasks. Routing Efficiency: The OSPF performance testing involves verification of its effectiveness in dynamic routing and route calculation as well as assessing convergence rate. Network Performance Testing: The test approach delineates network device performance in normal operation and under failure scenarios. ii. Test Scenarios The tests will verify operational ability of fundamental networking devices through various scenarios. • VLA N Configuration: Make sure devices in different VLANs are not connected to one another while communication is permitted only via appropriate routing mechanisms. • Firewall Rules: Make sur e devices in different VLANs are not connected to one another while communication is permitted only via appropriate routing mechanisms. • HSRP Redundancy: A test for HSRP Redundancy should b e performed to test the failover handover among routers in the event a failure occurs. • OSPF Routing: The OSPF must dynamicall y mirror the changes in network topology through efficient processing in maintaining routing tables. • ACLs Implementation: Acces s Control Lists implementation should be validated to allow for

efficient traffic filtering as well as access policy implementation. iii. Test Cases Testing will highlight particular tests per component of the configuration: • VLAN Isolation: Eac h network segment in different VLANs must not be allowed to communicate directly until there are appropriate routing configurations. •Firewall Policies: Different network traffic tests like HTTP, FTP, ICMP must pass through the firewall system while its rules properly permit or block communications. •HSR P Failover: Simulation of the failure of the primary router should be performed to verify that both the network performance is unaffected while the standby router assumes responsibility. •OSPF Convergence: Implementation of multiple OSPF convergence cases of router addition and deletion across the network should be verified for smooth and proper convergence processes. • AC Ls Implementation: Different ACL tests should be run in order to validate permitted user access to restricted network assets with appropriate checking for proper enforcement of security policy. The platform includes comprehensive security testing facilities by virtue of which the network can achieve proper functioning and fault-tolerant operation against anticipated risks. 1 2 3 5 Test Plan Table Why cannot we use VPN? 1 2 3 This scenario is not feasible for implementing VPN because the program of Cisco Packet Tracer lacks support to simulate VPN protocol features and encryption mechanisms. VPN is supported on the ASA device in real-world networks, but the test platform lacks the provision to accurately emulate VPN features hence testing and deployment of VPN is not practical. 1 4 Test Cases with Verification Connectivity Test Figure 27 Ping Successful Figure 28 Ping Unsuccessful VLAN and Inter-VLAN Connectivity Test Figure 29 Inter-VLAN Test Figure 30 DHCP Request Successful Figure 31 HSRP Test Firewall Test Figure 32 Firewall doesn’t allow unauthorized traffic Figure 33 Firewall allows authorized traffic

ACL Test Figure 34 : Specified devices communicate Figure 35 Unspecified devices don't communicate Servers Test Figure 36 DNS accessed by using domain Figure 37 Print server accessed Figure 38 File server accessed IP address table DHCP has been used to asign IP addresses. 1 M4 - Analysis of Test Results and Recommendations for Network Enhancements This section outlines the tests conducted in various network environments to identify infrastructure issues, resolve system defects, and suggest modifications to improve network performance, security, and dependability. 1 4 1. Physical and IP Connectivity Tests The tests ensured connectivity between same-subnet devices as well as between various subnets after routing has been configured. 4 Findings: Some devices established connections, and others failed because of defective IP addresses, defective cables, or ICMP requests being blocked by firewalls. 1 4 221 Recommendations: Check the physical connections and cables to ensure that they are correctly connected and not suffer from extreme signal loss, especially in the case of fiber optics. 1 Ensure that all equipment is properly set with the correct IP and subnet mask settings. Configure firewalls to allow ICMP requests without sacrificing security features. Check switch and router settings to solve routing issues and maintain error-free connections. 1 4 2. VLAN and Inter-VLAN Connectivity Tests This test validated communication within the same VLAN and between different VLANs. 1 Internal communication between VLAN 10 and connectivity to VLAN 20 were made. Risks: Unapproved VLAN traffic between VLANs and potential network congestion. 1 Recommendations: Regularly validate device VLAN assignments. 1 4 Implement VLAN Access Control Lists (VACLs) to restrict unauthorized VLAN traffic. Enable private VLANs to isolate sensitive devices. 1 4 Implement 802.1Q VLAN trunking and disable unused ports for improved security and efficiency. 1 3. Protocol Testing a. DHCP Test: The test examined the DHCP server to determine whether it could distribute valid IP addresses to

clients. Findings: IP address allocation was achieved, though IP conflicts or inadequate address pools might occur. Recommendations: Make sure the DHCP scope has sufficient IP addresses for all the clients. Utilize an IP Address Management (IPAM) system with conflict detection capabilities. Install redundant DHCP servers to provide a backup in the event of a failure. b. 1 4 6 14 15 21 29 176 HSRP Test This test tracked the failover process of the Hot Standby Router Protocol (HSRP) between the master and standby routers. 1 4 Findings: The failover did not work due to improper router priorities, standby router issues, and disabled interface tracking. Recommendations: Use proper HSRP priorities so that the master router has a higher priority value. 1 Enable the preempt option to allow automatic failback to the master router. Enable interface tracking for failover on link failure. Simulate failure scenarios to verify redundancy functionality. 24 174 184 191 192 4. Firewall Test The firewall test confirmed that unauthorized traffic was being blocked properly while valid traffic was being allowed. Findings: Unauthorized traffic was sometimes accidentally blocked. Recommendations: parallelely check and maintain firewall policies to balance security with accessibility. noenable logging and alarm functions to track abnormal activities in real time. ointegrate Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) for added security. 246 Use security zone segmentation (e.g., internal, external, DMZ) to enhance protection of sensitive network segments. 5. Access Control List (ACL) Test The ACL test checked blocking of unauthorized traffic and passing through of specific IP addresses. •Findings: The rules functioned properly, but very tight ACLs may block legitimate traffic. •Recommendations: Optimize rule order, keeping some rule s at the start to process them rapidly. Scheduled review and cleanup of ACLs to purge stale entries. Test access patterns against the test network to apply rules properly and avoid

spurious traffic blocks. 6. Server Testing a. DNS Server Test: The test verified domain name resolution functionality in clients. •Findings: Resolution functioned correctly, but possible risks involved were DNS server failures and DNS spoofing attacks. •Recommendations : Activate secondary DNS servers as backups. 107 Implement DNSSEC for authenticating authoritative DNS responses and protection against spoofing. Inspect DNS logs for alerting on suspicious access patterns or security problems. b. Print Server Test: The test confirmed print request management through the network print server. • Risks : Non-authorized printer access could lead to data invasion. • Recommendations: Apply role-based access controls to restrict printe r use to authorized staff members only. Schedule regular viewing of print logs for symptom discovery of unauthorized usage. Trace print queues with a high-priority assignment on mission-critical print jobs. c. File Server Test: Valid and invalid credentials were both tested against the file server in order to ensure authentication. Results: Authentication was done as expected, but the attempt at unauthorized access always poses a security risk. 1 220 Recommendations: Use multi-factor authentication (MFA) to protect sensitive files against access. 1 Encrypt sensitive information from unauthorized access. Periodically audit file accesses to spot any suspicious activity and respond appropriately. 1 2 3 VPN Testing Successful VPN connectivity testing was a major missing element that appeared as "False" in the test plan table pointing toward an urgent attention need. Summary Every test gave significant insights into how the network functions and pinpointed certain areas which could be optimized. The steps suggested are directed towards enhancing network efficiency, functionality, and security and overall operation process. 1 2 3 96 D2: Critical Evaluation of the Network Design, Planning, Configuration, and Testing Introduction The assessment considers the notion of design in the early planning stage and further

project configuration exercises alongside testing operations conducted in the new network environment. [1][2][3] The assessment includes network topology design and protocol tests alongside pre-implementation checking and post-implementation verification and configuration confirmation and testing methodology appraisal. [1] Building a stable network environment requires dealing with strength analysis and weakness diagnosis focusing on areas of potential growth as the imperative task. 1. Design & Planning Assessment Strengths: Network Architecture and Segmentation: The network layout ensures proper VLAN segregation between the student and teacher departments and the head department and server's sectors thus creating isolated network segments for better departmental security. Network growth in the future becomes easy due to the fact that multi-layered switches provide routing functions with advanced security capabilities which help achieve strong system immunity. Security Implementation: The network security solutions employed contain several defense layers. Points of entry security is guaranteed by access layer switches that impose departmental security policies. Multi-layer switches are vital network appliances as they integrate routing abilities with security components to enhance the inspection of traffic. ASA serves as a perimeter security device to monitor internal and external traffic flow. Grain-level traffic management with improved security is offered through applying the Access Control Lists (ACLs) protocol that inhibits unauthorized access attempts. Redundancy Factors: HSRP (Hot Standby Router Protocol) along with other High Availability features is implemented in the design to execute router failover operations thus ensuring reduced network downtime because of router failure. [1][2][3][5][10][26] OSPF (Open Shortest Path First) enables dynamic routing as part of its operation that ensures the network remains adaptable to changes and faults for offering fault-tolerant routing operations. [1] The architecture

design incorporates secondary switches to provide dependable departmental network connectivity by eliminating potential breakpoints. Weaknesses: Poor Initial Requirement Gathering: Business objectives may be in conflict with the network design because of inadequate documentation on initial requirements gathering and business needs assessment. Non-Scalability and Capacity Planning: Current network planning lacks specific plans that would identify increases in network capacity as well as opportunities for capacity expansion that would have an adverse impact on future expansion and user and traffic handling capacity. 1 Wireless Security Planning: The planning includes wireless access points but lacks security plans that would include WPA3 implementation as well as strong encryption and RADIUS authentication for wireless clients. 1 Absence of Disaster Recovery and Business Continuity Planning: Business objectives could fail to map on the network topology because of the lack of sufficient documentation concerning first-time requirements collection and business requirements analysis. 1 2. Configuration Evaluation Strengths: VLAN Configuration: The network segmentation is successful because the VLAN configuration deployed is thorough and well-implemented. 1 The department zones separate unauthorized data exchange between departments with no need to communicate. 1 2. DHCP Configuration: The DHCP configuration contains proper scope and exclusion configuration and an address pool that ensures client devices obtain network addresses from the specified area. 1 3. Core Services Implementation: The network facilitates name resolution as DNS servers were configured according to accurate setups. The print server system possesses correct functionality to provide printers as shared resources to relevant departments. The file server contains authentication protocols to protect access points while the database server is provided with accurate configuration for secure data handling and accessibility protocols. Weaknesses:

1. VPN Configuration Incomplete: Test results show that there is no complete or properly working VPN configuration. The lack of VPN configuration cannot provide secure network access for remote users thus posing an urgent security risk. 1 2. Incomplete Security Hardening: There are no documents guiding how the servers and devices can be hardened in the company against security threats. Best practices for security like disabling ports as well as applying firmware and security patch updates are not well documented. 3. Lack of QoS (Quality of Service) Configuration: The organization lacks QoS configuration policies for its business-critical services like VoIP and video conferencing systems that may result in poor quality of service or slowness at the time of heavy network traffic. 1 4. Backup Configuration Gaps: The documentation lacks clear reporting on backup configurations of server data and system configurations along with network setup. 1 System recovery is compromised when such failure occurs. 3. Testing Evaluation Strengths: 1. Structured Test Plan: The developed test plan has sound structure that demonstrates solid goals while extending to complete test cases that validate key network functionality areas: Thorough VLAN separation testing is needed for the validation of the proper segmentation configuration. The test ensured that all permitted access protocols were properly authorized through firewall rule testing. The test evaluates HSRP failover functionality because it validates network resilience against router failures. An experiment validated OSPF dynamic routing by confirming its setup status. Confirmation of security effects on traffic filtering includes testing the implementation of ACL. DNS and print, file and database servers were tested. 1 2. Comprehensive Documentation of Test Results: Test results generate detailed documentation with pass/ fail analysis methods to reveal system operations and security elements of the network. 1 Weaknesses: 1. Limited Scope of Security

Testing: The test process skips penetration testing and hence a lack of vulnerability analyses. 1 Vulnerability scanning and social engineering testing are not included in the program as they can expose attack surface weaknesses. 1 Physical security testing is required for all network infrastructures to find possible unauthorized access points. 2.Lack of Stress Testing: The system is not subjected to high traffic performance testing and therefore limiting awareness of its maximum capacity and scalability possibilities. Employee safety would be at risk because important file and database servers lack documentation for verifying their functionality in case of a failover situation. 3. Test Documentation Gaps: Absence of detailed metrics along with quantitative data in test results restricts full performance analysis of the network. Insufficient documentation of the test environment configuration makes it less easy to reproduce test results. 1 Failed tests lack remediation plans so the identified issues from testing might have delayed resolutions. 4. Critical Recommendations 1. 1 Security Enhancements: •VPN Deployment: Organizations must finish testing and deploying VPN solutions to provide remote access security using the deployed VPN system. •IDS/IPS Systems: ID S/IPS Systems must be deployed to improve network security through real-time threat detection by providing both Intrusion Detection/Prevention Systems capabilities. •Security Hardening: A security hardening process must be developed for network devices and servers which will help reduce their vulnerabilities. • Netwo rk Monitoring and Logging: There should be a mechanism of constant network monitoring with centralized logging to perform real-time incident detection. 1 2. Testing Improvements: Automated Testing Tools: Automated testing tools enable the users to perform performance benchmarking as well as regression testing for continuous network functionality. 1 Penetration Testing: Penetration

testers should be executed regularly to find penetrable weak points which allow attackers into the network and test its defense mechanism. 1 Stress and Scalability Testing: High traffic stress tests should be performed with the addition of scalability tests to confirm network capacity for growth. 1 Disaster Recovery Testing: Full disaster recovery testing procedures should be established by the organization to confirm verification of the network systems as well as data can be restored in the event of disasters. 3. Documentation Improvements: Network Topology Documentation: Network topology documentation requires thorough detailed improvements to yield transparency through easier troubleshooting and management processes. 1 Configuration Management: The plan should include configuration management elements such as configuration version control and complete change logs for configuration records. 1 Change Management Processes: The organization should develop systematic change management processes to maintain configuration consistency as well as avoid update errors. Incident Response Procedures: Documented procedures for responding to security breaches and network failure incidents should be developed by the company. 1 4. Infrastructure Improvements: Critical Service Redundancy: Through the implementation of critical service redundancy by the deployment of backup DNS DHCP file servers, fault tolerance and system availability will be increased. QoS for Critical Applications: Quality of Service (QoS) configurations should be implemented to set up priority traffic rules for applications with low latency requirements like VoIP to optimize operational performance. 1 Monitoring Improvements: The network monitoring should be increased for real-time traffic observation and alerting facilities and precise resource utilization monitoring. Backup and Recovery Solutions: The organization should have full backup procedures for mission-critical applications using offsite storage, which automatically performs recovery procedures. 5. Process

Improvements: Periodic Security Audits: The network needs to have periodic security audits as part of a routine assessment schedule to monitor its security position. Staff Training Programs: The organization has to carry out Staff Training Programs that enhance security skills as well as network management and incident response skills among the staff. Regular Testing Schedules: The institution has to have fixed time intervals for conducting performance testing in addition to security audits and scalability testing to ensure network functionality. Incident Response Drills: The group should carry out periodic incident response drills that prepare them with the ability to react suitably to actual attack incidents. 5. Overall Assessment Numerous departments will take advantage of the strong network architecture that creates sound traffic segmentation with the help of good routing and proper security deployment. The proposed network contains multiple vital flaws which compromise its future operational reliability and scalability along with security threats. Network security is under significant risk because VPN settings are not completed, and there are no disaster recovery plans alongside poor security test scope. 1 Appendix: Presentation: 1 References: Zhou, L. and Xu, L. (2020) Cybersecurity in the Modern Age: Issues and Solutions. London: Elsevier. 1 2 Scarfone, K. and Mell, P. (2019) Guide to Intrusion Detection and Prevention Systems (IDPS). 1 Wireshark Foundation. (2024) Wireshark (Version 4.0. 1) [Software]. Available at: https://www.wireshark.org (Accessed: 16 February 2025). Tan, K. and Chen, Y. (2022) Advanced Network Security: Threats, Attacks, and Countermeasures. New York: Wiley. Kent, S. and Seo, K. (2005) Security Architecture for the Internet Protocol. 1 4 Menezes, A. J., van Oorschot, P. C. and Vanstone, S. A. (1996) Handbook of Applied Cryptography. 1 7 Boca Raton, FL: CRC Press. 1 3 6 Stallings, W. (2020) Network Security Essentials: Applications and Standards (6th ed.). 1 3 Pearson. 1 Baker,

T. (2020) Network Security Technologies and Tools. 2nd ed. Chicago: Pearson. Netwrix. (2019) ‘Network security devices you need to know about’. Netwrix Blog. Zhang, Y. and M. M. (2021) Cloud Computing and Security: Challenges and Future Directions. OWASP. (n.d.) ‘OWASP Foundation: Leading Application Security’. Available at: https://owasp.org (Accessed: 16 February 2025). 15 Dierks, T. and Rescorla, E. (2008) The Transport Layer Security (TLS) Protocol. 1 Ylonen, T. and Lonvick, C. (2006) The Secure Shell (SSH) Protocol Architecture. Cisco Systems. (2023) ‘What is network security?’. Cisco. Liu, H., Wang, L. and Zhang, T. (2021) ‘Artificial Intelligence in Network Security: A Survey’. Journa l of Network and Computer Applications, 160, pp. 102602. https:/ /doi.org/10.1016/j.jnca.2020.102602. Zenarmor. (2023) ‘Network securit y devices’. Zenarmor. Harris, S. (2019) CISSP All-in-One Exam Guide (8th ed.). 1 New York: McGraw-Hill. 1 Kizza, J. (2020) Guide to Computer Network Security (4th ed.). 1 Cham: Springer. 1 MITRE. (n.d.) ‘MITRE Corporation: Delivering Security Solutions’. 1 Available at: https:/ /mitre.org (Accessed: 16 February 2025). 12 Scarfone, K. and Mell, P. (2019) Guide to Intrusion Detection and Prevention Systems (IDPS).

REPORT #24825067

Results

Sources that matched your submitted document.

IDENTICAL CHANGED TEXT

1.	EXTERNAL DATABASE 62.63% ISMT College - 16 Feb 2025, 2:43 AM	IDENTICAL CHANGED TEXT
2.	EXTERNAL DATABASE 21.12% ISMT College - 15 Feb 2025, 10:25 PM	IDENTICAL CHANGED TEXT
3.	EXTERNAL DATABASE 20.98% ISMT College - 15 Feb 2025, 10:46 PM	IDENTICAL CHANGED TEXT
4.	EXTERNAL DATABASE 17.46% ISMT College - 15 Feb 2025, 10:27 AM	IDENTICAL CHANGED TEXT
5.	EXTERNAL DATABASE 4.91% ISMT College - 15 Feb 2025, 1:05 PM	IDENTICAL CHANGED TEXT
6.	EXTERNAL DATABASE 3.1% ISMT College - 18 Jul 2024, 11:49 PM	CHANGED TEXT
7.	EXTERNAL DATABASE 2.55% ISMT College - 23 Jan 2025, 11:13 AM	CHANGED TEXT
8.	EXTERNAL DATABASE 2.54% ISMT College - 8 Jan 2024, 9:48 PM	CHANGED TEXT
9.	EXTERNAL DATABASE 2.54% ISMT College - 21 Dec 2024, 8:28 AM	IDENTICAL CHANGED TEXT

REPORT #24825067

EXTERNAL DATABASE
10. 2.53% ISMT College - 23 Nov 2024, 11:57 AM

EXTERNAL DATABASE
11. 2.51% ISMT College - 13 Aug 2024, 4:37 AM

EXTERNAL DATABASE
12. 2.51% ISMT College - 28 Aug 2024, 9:48 PM

EXTERNAL DATABASE
13. 2.47% ISMT College - 14 Aug 2024, 2:18 AM

EXTERNAL DATABASE
14. 2.45% ISMT College - 15 Feb 2025, 9:11 AM

EXTERNAL DATABASE
15. 2.44% ISMT College - 15 Feb 2025, 11:20 PM

EXTERNAL DATABASE
16. 2.43% ISMT College - 28 Aug 2024, 10:40 AM

EXTERNAL DATABASE
17. 2.41% ISMT College - 28 Aug 2024, 9:42 PM

EXTERNAL DATABASE
18. 2.41% ISMT College - 18 Jan 2024, 8:30 AM

EXTERNAL DATABASE
19. 2.39% ISMT College - 27 Nov 2023, 11:44 AM

EXTERNAL DATABASE
20. 2.38% ISMT College - 23 Nov 2024, 11:32 AM

REPORT #24825067

EXTERNAL DATABASE
21. 2.38% ISMT College - 12 May 2024, 12:25 PM

EXTERNAL DATABASE
22. 2.38% ISMT College - 15 Aug 2024, 12:06 AM

EXTERNAL DATABASE
23. 2.38% ISMT College - 19 Dec 2024, 11:35 AM

EXTERNAL DATABASE
24. 2.35% ISMT College - 27 Nov 2024, 9:10 AM

EXTERNAL DATABASE
25. 2.35% ISMT College - 15 May 2024, 11:17 AM

EXTERNAL DATABASE
26. 2.31% ISMT College - 11 Feb 2025, 12:38 AM

EXTERNAL DATABASE
27. 2.3% ISMT College - 7 Feb 2025, 4:36 AM

EXTERNAL DATABASE
28. 2.29% ISMT College - 14 Feb 2025, 1:51 AM

EXTERNAL DATABASE
29. 2.29% ISMT College - 23 Nov 2024, 11:36 AM

EXTERNAL DATABASE
30. 2.28% ISMT College - 23 Nov 2024, 1:49 AM

EXTERNAL DATABASE
31. 2.27% ISMT College - 24 Nov 2024, 2:43 AM

REPORT #24825067

EXTERNAL DATABASE
32. 2.27% ISMT College - 7 Dec 2024, 9:55 AM

EXTERNAL DATABASE
33. 2.26% ISMT College - 11 Aug 2024, 9:40 PM

EXTERNAL DATABASE
34. 2.26% ISMT College - 23 Nov 2024, 8:25 AM

EXTERNAL DATABASE
35. 2.26% ISMT College - 27 Nov 2023, 8:37 AM

EXTERNAL DATABASE
36. 2.26% ISMT College - 29 Aug 2024, 10:50 AM

EXTERNAL DATABASE
37. 2.25% ISMT College - 13 Jun 2023, 3:51 AM

EXTERNAL DATABASE
38. 2.24% ISMT College - 23 Nov 2024, 2:18 AM

EXTERNAL DATABASE
39. 2.22% ISMT College - 28 Dec 2024, 9:14 PM

EXTERNAL DATABASE
40. 2.22% ISMT College - 11 Jul 2024, 7:03 AM

EXTERNAL DATABASE
41. 2.22% ISMT College - 29 Aug 2024, 6:42 AM

EXTERNAL DATABASE
42. 2.2% ISMT College - 19 Dec 2024, 7:03 AM

REPORT #24825067

EXTERNAL DATABASE
43. 2.19% ISMT College - 29 Aug 2024, 10:25 AM

EXTERNAL DATABASE
44. 2.19% ISMT College - 20 May 2024, 11:46 AM

EXTERNAL DATABASE
45. 2.19% ISMT College - 12 May 2024, 7:25 AM

EXTERNAL DATABASE
46. 2.19% ISMT College - 24 May 2023, 8:41 AM

EXTERNAL DATABASE
47. 2.18% ISMT College - 27 Dec 2024, 5:11 AM

EXTERNAL DATABASE
48. 2.18% ISMT College - 4 Jul 2023, 1:12 AM

EXTERNAL DATABASE
49. 2.18% ISMT College - 11 Jun 2023, 11:12 PM

EXTERNAL DATABASE
50. 2.17% ISMT College - 4 Jan 2025, 4:42 AM

EXTERNAL DATABASE
51. 2.16% ISMT College - 3 Jul 2023, 10:07 PM

EXTERNAL DATABASE
52. 2.16% ISMT College - 23 Nov 2024, 3:35 AM

EXTERNAL DATABASE
53. 2.16% ISMT College - 19 Dec 2024, 3:50 AM

REPORT #24825067

EXTERNAL DATABASE
54. 2.16% ISMT College - 12 May 2024, 1:46 AM

EXTERNAL DATABASE
55. 2.15% ISMT College - 17 May 2024, 4:37 AM

EXTERNAL DATABASE
56. 2.14% ISMT College - 6 Feb 2025, 6:20 AM

EXTERNAL DATABASE
57. 2.14% ISMT College - 8 Oct 2024, 11:45 PM

EXTERNAL DATABASE
58. 2.14% ISMT College - 11 Dec 2024, 9:39 AM

EXTERNAL DATABASE
59. 2.13% ISMT College - 28 Dec 2024, 7:59 AM

EXTERNAL DATABASE
60. 2.13% ISMT College - 13 Aug 2024, 8:52 AM

EXTERNAL DATABASE
61. 2.12% ISMT College - 9 Jul 2024, 4:06 AM

EXTERNAL DATABASE
62. 2.12% ISMT College - 23 Nov 2024, 11:20 AM

EXTERNAL DATABASE
63. 2.12% ISMT College - 3 Sep 2024, 3:20 AM

EXTERNAL DATABASE
64. 2.12% ISMT College - 12 May 2024, 12:02 AM

REPORT #24825067

EXTERNAL DATABASE
65. 2.11% ISMT College - 15 Aug 2024, 6:05 AM

EXTERNAL DATABASE
66. 2.11% ISMT College - 27 Sep 2024, 11:06 AM

EXTERNAL DATABASE
67. 2.1% ISMT College - 15 Aug 2024, 12:45 PM

EXTERNAL DATABASE
68. 2.1% ISMT College - 27 Aug 2024, 11:48 AM

EXTERNAL DATABASE
69. 2.1% ISMT College - 14 Aug 2024, 2:31 AM

EXTERNAL DATABASE
70. 2.1% ISMT College - 28 Mar 2024, 9:23 AM

EXTERNAL DATABASE
71. 2.09% ISMT College - 4 Sep 2024, 4:01 AM

EXTERNAL DATABASE
72. 2.09% ISMT College - 15 May 2024, 1:07 PM

EXTERNAL DATABASE
73. 2.09% ISMT College - 6 May 2024, 4:51 AM

EXTERNAL DATABASE
74. 2.08% ISMT College - 11 Oct 2023, 3:28 AM

EXTERNAL DATABASE
75. 2.08% ISMT College - 5 Feb 2025, 1:46 AM

REPORT #24825067

EXTERNAL DATABASE
76. 2.08% ISMT College - 12 May 2024, 3:34 AM

EXTERNAL DATABASE
77. 2.07% ISMT College - 23 Nov 2024, 9:28 AM

EXTERNAL DATABASE
78. 2.07% ISMT College - 26 Dec 2024, 6:19 AM

EXTERNAL DATABASE
79. 2.07% ISMT College - 24 May 2023, 9:08 AM

EXTERNAL DATABASE
80. 2.07% ISMT College - 27 Oct 2024, 9:50 AM

EXTERNAL DATABASE
81. 2.06% ISMT College - 15 Sep 2024, 10:57 AM

EXTERNAL DATABASE
82. 2.06% ISMT College - 8 Feb 2025, 12:06 AM

EXTERNAL DATABASE
83. 2.06% ISMT College - 3 Jun 2024, 11:48 PM

EXTERNAL DATABASE
84. 2.05% ISMT College - 3 Aug 2024, 2:02 AM

EXTERNAL DATABASE
85. 2.05% ISMT College - 19 Jan 2025, 10:13 PM

EXTERNAL DATABASE
86. 2.05% ISMT College - 7 Feb 2025, 6:44 AM

REPORT #24825067

EXTERNAL DATABASE
87. 2.04% ISMT College - 1 Apr 2024, 4:53 AM

EXTERNAL DATABASE
88. 2.04% ISMT College - 23 Mar 2023, 5:42 AM

EXTERNAL DATABASE
89. 2.04% ISMT College - 26 Nov 2024, 4:03 AM

EXTERNAL DATABASE
90. 2.04% ISMT College - 15 Jun 2024, 4:14 AM

EXTERNAL DATABASE
91. 2.04% ISMT College - 9 Aug 2024, 12:19 AM

EXTERNAL DATABASE
92. 2.04% ISMT College - 4 May 2024, 2:50 AM

EXTERNAL DATABASE
93. 2.03% ISMT College - 16 Feb 2025, 4:31 AM

EXTERNAL DATABASE
94. 2.03% ISMT College - 13 Jun 2023, 10:52 PM

EXTERNAL DATABASE
95. 2.03% ISMT College - 8 Feb 2025, 3:56 AM

EXTERNAL DATABASE
96. 2.02% ISMT College - 31 Jan 2025, 11:08 AM

EXTERNAL DATABASE
97. 2.02% ISMT College - 25 Nov 2024, 2:08 AM

REPORT #24825067

EXTERNAL DATABASE

98. 2.02% ISMT College - 7 Feb 2025, 10:23 AM

EXTERNAL DATABASE

99. 2.02% ISMT College - 17 Nov 2023, 12:47 AM

100.

EXTERNAL DATABASE

2.01% ISMT College - 8 Mar 2024, 12:47 PM

101.

EXTERNAL DATABASE

2.01% ISMT College - 13 Aug 2024, 6:27 AM

102.

EXTERNAL DATABASE

2.01% ISMT College - 8 Feb 2025, 9:37 AM

103.

EXTERNAL DATABASE

2.01% ISMT College - 18 Sep 2024, 2:05 AM

104.

EXTERNAL DATABASE

2.01% ISMT College - 22 Nov 2024, 3:00 PM

105.

EXTERNAL DATABASE

2.01% ISMT College - 14 Aug 2024, 6:41 AM

106.

EXTERNAL DATABASE

2.01% ISMT College - 19 May 2024, 11:50 AM

107.

EXTERNAL DATABASE

2.01% ISMT College - 3 Jun 2024, 5:36 AM

108.

EXTERNAL DATABASE

2% ISMT College - 6 Oct 2024, 9:59 PM

109.
EXTERNAL DATABASE
2% ISMT College - 4 Feb 2025, 5:04 AM

110.
EXTERNAL DATABASE
1.99% ISMT College - 21 Jul 2024, 7:24 AM

111.
EXTERNAL DATABASE
1.98% ISMT College - 15 Aug 2024, 9:19 AM

112.
EXTERNAL DATABASE
1.98% ISMT College - 19 Jan 2025, 10:04 PM

113.
EXTERNAL DATABASE
1.98% ISMT College - 12 Sep 2024, 1:12 PM

114.
EXTERNAL DATABASE
1.98% ISMT College - 26 Apr 2024, 10:42 AM

115.
EXTERNAL DATABASE
1.97% ISMT College - 8 Feb 2025, 9:47 AM

116.
EXTERNAL DATABASE
1.96% ISMT College - 23 Nov 2024, 8:30 AM

117.
EXTERNAL DATABASE
1.96% ISMT College - 14 Aug 2024, 9:41 AM

118.
EXTERNAL DATABASE
1.96% ISMT College - 13 Aug 2024, 10:51 PM

119.
EXTERNAL DATABASE
1.96% ISMT College - 5 Jul 2023, 10:[illegible] AM

120.
EXTERNAL DATABASE
1.95% ISMT College - 8 Feb 2025, 5:22 AM

121.
EXTERNAL DATABASE
1.95% ISMT College - 13 Aug 2024, 12:57 AM

122.
EXTERNAL DATABASE
1.95% ISMT College - 4 Oct 2024, 1:47 AM

123.
EXTERNAL DATABASE
1.95% ISMT College - 19 Jun 2023, 11:54 AM

124.
EXTERNAL DATABASE
1.94% ISMT College - 17 Jun 2023, 12:03 AM

125.
EXTERNAL DATABASE
1.94% ISMT College - 4 May 2024, 3:21 AM

126.
EXTERNAL DATABASE
1.94% ISMT College - 11 Jun 2023, 11:32 AM

127.
EXTERNAL DATABASE
1.94% ISMT College - 16 Jan 2025, 10:10 AM

128.
EXTERNAL DATABASE
1.94% ISMT College - 1 Sep 2024, 9:51 PM

129.
EXTERNAL DATABASE
1.93% ISMT College - 23 May 2023, 11:57 PM

130.
EXTERNAL DATABASE
1.93% ISMT College - 21 Dec 2024, 8:31 AM

REPORT #24825067

131.
EXTERNAL DATABASE
1.93% ISMT College - 18 Jan 2025, 10:08 PM

132.
EXTERNAL DATABASE
1.93% ISMT College - 4 Nov 2023, 5:17 AM

133.
EXTERNAL DATABASE
1.93% ISMT College - 6 Jul 2023, 1:59 PM

134.
EXTERNAL DATABASE
1.92% ISMT College - 12 Dec 2024, 9:30 AM

135.
EXTERNAL DATABASE
1.91% ISMT College - 13 Mar 2024, 12:47 PM

136.
EXTERNAL DATABASE
1.91% ISMT College - 23 May 2023, 4:30 PM

137.
EXTERNAL DATABASE
1.91% ISMT College - 19 May 2024, 3:30 AM

138.
EXTERNAL DATABASE
1.9% ISMT College - 4 Jan 2025, 10:01 PM

139.
EXTERNAL DATABASE
1.9% ISMT College - 12 Dec 2024, 12:02 PM

140.
EXTERNAL DATABASE
1.9% ISMT College - 8 Feb 2025, 12:31 AM

141.
EXTERNAL DATABASE
1.9% ISMT College - 31 Jan 2025, 5:[illegible] AM

REPORT #24825067

142.
EXTERNAL DATABASE
1.89% ISMT College - 18 Dec 2024, 8:03 AM

143.
EXTERNAL DATABASE
1.88% ISMT College - 16 Feb 2025, 12:08 AM

144.
EXTERNAL DATABASE
1.88% ISMT College - 20 Oct 2024, 4:13 AM

145.
EXTERNAL DATABASE
1.88% ISMT College - 20 May 2024, 2:40 AM

146.
EXTERNAL DATABASE
1.88% ISMT College - 4 Jul 2023, 1:13 AM

147.
EXTERNAL DATABASE
1.88% ISMT College - 7 Jul 2023, 1:01 AM

148.
EXTERNAL DATABASE
1.84% ISMT College - 29 Aug 2024, 3:48 AM

149.
EXTERNAL DATABASE
1.83% ISMT College - 19 Dec 2024, 10:27 AM

150.
EXTERNAL DATABASE
1.81% ISMT College - 6 Dec 2024, 11:44 AM

151.
INTERNET SOURCE
1.8% www.studocu.com

152.
EXTERNAL DATABASE
1.8% ISMT College - 21 May 2023, 1:39 AM

153.
EXTERNAL DATABASE
1.79% ISMT College - 19 Jun 2023, 5:46 AM

154.
EXTERNAL DATABASE
1.78% ISMT College - 2 Aug 2024, 3:52 AM

155.
EXTERNAL DATABASE
1.76% ISMT College - 12 Oct 2023, 7:40 AM

156.
EXTERNAL DATABASE
1.76% ISMT College - 21 Nov 2023, 9:05 AM

157.
EXTERNAL DATABASE
1.74% ISMT College - 28 May 2024, 9:14 PM

158.
EXTERNAL DATABASE
1.68% ISMT College - 5 Nov 2023, 10:26 AM

159.
EXTERNAL DATABASE
1.68% ISMT College - 1 Sep 2024, 9:51 PM

160.
EXTERNAL DATABASE
1.67% ISMT College - 21 Nov 2023, 9:30 AM

161.
EXTERNAL DATABASE
1.66% ISMT College - 25 Sep 2024, 8:08 AM

162.
EXTERNAL DATABASE
1.62% ISMT College - 5 Aug 2024, 9:57 AM

163.
EXTERNAL DATABASE
1.58% ISMT College - 8 Sep 2023, 8:[illegible] AM

REPORT #24825067

164.
EXTERNAL DATABASE
1.54% ISMT College - 5 Jul 2024, 8:35 AM

165.
EXTERNAL DATABASE
1.46% ISMT College - 19 May 2024, 3:06 PM

166.
EXTERNAL DATABASE
1.44% ISMT College - 18 Dec 2024, 8:44 AM

167.
EXTERNAL DATABASE
1.37% ISMT College - 14 Nov 2024, 7:30 AM

168.
EXTERNAL DATABASE
1.2% ISMT College - 5 Jul 2024, 7:53 AM

169.
EXTERNAL DATABASE
0.87% ISMT College - 9 Feb 2025, 5:23 AM

170.
INTERNET SOURCE
0.86% www.tcpwave.com
https://www.tcpwave.com/twc-glossary/

171.
EXTERNAL DATABASE
0.74% ISMT College - 10 Mar 2023, 5:20 AM

172.
EXTERNAL DATABASE
0.73% ISMT College - 21 Apr 2024, 6:47 AM

173.
INTERNET SOURCE
0.65% anonymityanywhere.com

https://anonymityanywhere.com/the-evolution-of-vpn-technology-a-timeline/

174.
EXTERNAL DATABASE
0.63% ISMT College - 25 Nov 2024, 11:08 PM

175.
EXTERNAL DATABASE
0.63% ISMT College - 10 Mar 2023, 2:12 AM

176.
EXTERNAL DATABASE
0.62% ISMT College - 5 Jan 2025, 3:38 AM

177.
EXTERNAL DATABASE
0.6% ISMT College - 21 Sep 2024, 1:55 AM

178.
EXTERNAL DATABASE
0.58% ISMT College - 10 Mar 2023, 2:12 AM

179.
EXTERNAL DATABASE
0.57% ISMT College - 10 Feb 2025, 1:24 AM

180.
INTERNET SOURCE
0.55% www.certexams.com
https://www.certexams.com/Blog/job-roles-and-interview-questions-for-certifie...

181.
INTERNET SOURCE
0.52% yingo.ca
https://yingo.ca/articles/the-ultimate-cryptography-guide-everything-you-need...

182.
EXTERNAL DATABASE
0.51% ISMT College - 14 Feb 2025, 10:56 PM

183.
EXTERNAL DATABASE
0.5% ISMT College - 21 Mar 2023, 9:50 AM

184.
EXTERNAL DATABASE

0.5% ISMT College - 26 Nov 2024, 3:57 AM

185.
EXTERNAL DATABASE
0.43% ISMT College - 11 Mar 2023, 11:48 PM

186.
INTERNET SOURCE
0.42% techtimes.uk
https://techtimes.uk/basics-of-cyber-security/

187.
INTERNET SOURCE
0.4% yingo.ca
https://yingo.ca/articles/cryptography-and-network-security-keeping-data-safe…

188.
INTERNET SOURCE
0.39% www.pillarsupport.com
https://www.pillarsupport.com/category/it-support/

189.
INTERNET SOURCE
0.39% giraffestudioapps.com
https://giraffestudioapps.com/cybersecurity-for-enterprises-2/

190.
INTERNET SOURCE
0.38% www.codelivly.com
https://www.codelivly.com/mastering-network-security-defending-against-cybe…

191.
EXTERNAL DATABASE
0.37% ISMT College - 26 Nov 2024, 12:32 AM

192.
EXTERNAL DATABASE
0.37% ISMT College - 27 Nov 2024, 9:15 AM

193.
EXTERNAL DATABASE
0.36% ISMT College - 21 Mar 2023, 9:50 AM

194.
INTERNET SOURCE
0.35% www.softwareseni.com

https://www.softwareseni.com/securing-user-data-techniques-and-tools/

195.
EXTERNAL DATABASE
0.31% ISMT College - 25 Aug 2024, 10:58 AM

197.
EXTERNAL DATABASE
0.29% ISMT College - 14 Aug 2024, 11:18 PM

198.
INTERNET SOURCE
0.28% cbtsys.com
http://cbtsys.com/online-training/it-training/Cisco-CCNA-Security.asp

199.
EXTERNAL DATABASE
0.28% ISMT College - 13 Oct 2023, 1:20 PM

200.
INTERNET SOURCE
0.27% datatracker.ietf.org
https://datatracker.ietf.org/doc/rfc6272/

201.
INTERNET SOURCE
0.27% tomsreviewbox.com
https://tomsreviewbox.com/wpaardhy/what-are-the-latest-advances-in-encrypt...

202.
EXTERNAL DATABASE
0.27% ISMT College - 4 Jan 2025, 6:08 AM

203.
EXTERNAL DATABASE
0.27% ISMT College - 28 Jan 2025, 4:19 AM

204.
INTERNET SOURCE
0.26% www.researchgate.net
https://www.researchgate.net/topic/Computer-Security

205.
EXTERNAL DATABASE
0.26% ISMT College - 27 Jul 2023, 4:46 AM

206.
INTERNET SOURCE
0.25% www.expensivity.com
https://www.expensivity.com/financial-v-election-fraud-and-security/

207.
INTERNET SOURCE
0.25% nigeriacodingacademy.com
https://nigeriacodingacademy.com/cryptography-for-ethical-hackers/

208.
INTERNET SOURCE
0.24% www.webasha.com
https://www.webasha.com/blog/common-ccna-interview-questions

209.
INTERNET SOURCE
0.22% cybsoftware.com
https://cybsoftware.com/how-organizations-can-secure-their-enterprise-traffic-…

210.
EXTERNAL DATABASE
0.22% ISMT College - 4 Oct 2024, 11:05 AM

211.
EXTERNAL DATABASE
0.21% ISMT College - 9 Mar 2023, 10:12 AM

212.
EXTERNAL DATABASE
0.2% ISMT College - 22 Mar 2023, 12:16 AM

213.
EXTERNAL DATABASE
0.2% ISMT College - 11 Feb 2025, 11:40 AM

214.
INTERNET SOURCE
0.17% tavoq.com
https://tavoq.com/blog/what-information-security-analyst-what-do-they-do

215.
EXTERNAL DATABASE
0.16% ISMT College - 19 Jan 2025, 7:43 AM

216.
EXTERNAL DATABASE
0.16% ISMT College - 8 Feb 2025, 1:42 AM

INTERNET SOURCE

217.
INTERNET SOURCE
0.15% beencrypted.com
https://beencrypted.com/encryption-guide/what-is-encryption/

218.
INTERNET SOURCE
0.15% www.thoughtfulviews.com
https://www.thoughtfulviews.com/2024/11/cyber-threat-prevention-how-to-saf...

219.
INTERNET SOURCE
0.15% ms.codes
https://ms.codes/blogs/internet-security/define-firewall-antivirus-and-antispyw...

220.
INTERNET SOURCE
0.15% payrollpayouts.com
https://payrollpayouts.com/payroll-software/

221.
INTERNET SOURCE
0.14% network-insight.net
https://network-insight.net/tag/conversational-learning/

222.
INTERNET SOURCE
0.14% www.yourcomputer.in
https://www.yourcomputer.in/how-to-secure-active-directory/

223.
INTERNET SOURCE
0.14% anonymityanywhere.com
https://anonymityanywhere.com/what-does-a-vpn-do/

224.
INTERNET SOURCE
0.14% softwareg.com.au
https://softwareg.com.au/blogs/internet-security/difference-between-firewall-a...

225.
INTERNET SOURCE
0.13% certknight.com
https://certknight.com/cisco-350-501-implementing-and-operating-cisco-servic...

226.
INTERNET SOURCE
0.13% marketbrew.ai
https://marketbrew.ai/the-benefits-of-ssl-tls-encryption-for-seo

227.
INTERNET SOURCE
0.13% www.certauri.com
https://www.certauri.com/unlocking-encryption-best-practices-for-secure-data…

228.
INTERNET SOURCE
0.13% yoho.cloud
https://yoho.cloud/blog/best-cloud-service-providers-in-nepal/

230.
INTERNET SOURCE
0.13% www.dontwatchme.com
https://www.dontwatchme.com/what-are-network-protocols/

229.
INTERNET SOURCE
0.13% www.tech2geek.net
https://www.tech2geek.net/understanding-the-four-types-of-network-services/

231.
INTERNET SOURCE
0.13% www.sentinelone.com
https://www.sentinelone.com/cybersecurity-101/cybersecurity/hashing/

232.
EXTERNAL DATABASE
0.13% ISMT College - 19 Dec 2024, 5:17 AM

233.
EXTERNAL DATABASE
0.13% ISMT College - 21 Oct 2024, 7:41 AM

234.
INTERNET SOURCE
0.12% network-insight.net
https://network-insight.net/tag/computer-networking/

235.
INTERNET SOURCE
0.12% www.globallegalpost.com
https://www.globallegalpost.com/lawoverborders/artificial-intelligence-154973…

236.
INTERNET SOURCE
0.12% similardifferent.com
https://similardifferent.com/difference-between-signature-and-hash/

237.
EXTERNAL DATABASE
0.12% ISMT College - 11 Sep 2024, 12:49 PM

238.
INTERNET SOURCE
0.11% secureitconsult.com

https://secureitconsult.com/network-security-management/

239.
INTERNET SOURCE
0.11% yingo.ca
https://yingo.ca/articles/understanding-cryptographic-services-the-essential-gu...

241.
INTERNET SOURCE
0.1% goo.by
https://goo.by/blog/everything-you-need-to-know-about-ip-troubleshooting-tip...

0.11% thinktechview.in
https://thinktechview.in/what-is-the-zero-trust-security-model/

242.
INTERNET SOURCE
0.1% www.hackersmexicanos.com
https://www.hackersmexicanos.com/exploring-the-importance-of-web-applicat...

243.
INTERNET SOURCE
0.09% resumeworded.com
https://resumeworded.com/interview-questions/network-administrator

244.
INTERNET SOURCE
0.09% www.clonedsgn.us
https://www.clonedsgn.us/business-it-infrastructure/

245.
INTERNET SOURCE
0.08% www.logon2tech.com
https://www.logon2tech.com/2023/01/complete-guide-to-soc-analyst-roles-skil...

246.
INTERNET SOURCE
0.08% indiafreenotes.com
https://indiafreenotes.com/tag/e-commerce-payment-gateways/

247.
INTERNET SOURCE
0.07% responsible-cyber-academy.com
https://responsible-cyber-academy.com/enhancing-your-cybersecurity-posture...

248.
INTERNET SOURCE
0.07% www.clonedsgn.us
https://www.clonedsgn.us/business-network-management/

249.
INTERNET SOURCE
0.06% blindbrowser.com
https://blindbrowser.com/mastering-internet-security-a-comprehensive-guide-t...

250.
INTERNET SOURCE
0.06% techtimes.uk
https://techtimes.uk/cyber-security-best-practices/

251.
EXTERNAL DATABASE
INTERNET SOURCE
0.06% ISMT College - 7 Jan 2025, 4:53 AM

252.
EXTERNAL DATABASE
0.06% ISMT College - 20 Oct 2024, 2:47 PM

253.
INTERNET SOURCE
0.05% www.expressvpn.com
https://www.expressvpn.com/blog/internet-security-technical-glossary/

REFERENCES

1. EXTERNAL DATABASE
1.54% ISMT College - 16 Feb 2025, 2:43 AM

2. INTERNET SOURCE
0.14% isj.vn
https://isj.vn/index.php/journal_STIS/article/view/118

3. EXTERNAL DATABASE
0.07% ISMT College - 8 Feb 2025, 9:37 AM

4. EXTERNAL DATABASE
0.07% ISMT College - 26 Dec 2024, 6:19 AM

5. INTERNET SOURCE
0.06% nvlpubs.nist.gov
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-146.pdf

6. EXTERNAL DATABASE
0.06% ISMT College - 23 Nov 2024, 11:08 AM

7. INTERNET SOURCE
0.02% en.wikipedia.org
https://en.wikipedia.org/wiki/Denial-of-service_attack