# FOUNDATIONS OF CYBERSECURITY:

**Summary of Knowledge and Skills Gained:**

1. **Understanding Cybersecurity Fundamentals:**
   * Learned the basic terminologies in cybersecurity, including key concepts like confidentiality, integrity, and availability (CIA triad), security controls, frameworks, and compliance standards (e.g., PCI DSS, GDPR, HIPAA).
   * Gained a clear understanding of various threat actors, including advanced persistent threats (APTs), insider threats, hacktivists, and their motivations.
2. **Familiarity with Common Threats and Attacks:**
   * Explored various types of attacks, such as phishing (e.g., spear phishing, vishing, smishing), malware (e.g., ransomware, spyware, worms), and social engineering techniques (e.g., USB baiting, watering hole attacks).
   * Developed an understanding of the psychology and manipulation techniques used by threat actors to exploit human error.
3. **Introduction to Security Tools and Techniques:**
   * Hands-on exposure to tools like SIEM systems, intrusion detection systems (IDS), and network protocol analyzers (e.g., packet sniffers like tcpdump).
   * Learned about encryption methods to secure data and protect it from unauthorized access.
   * Studied programming basics and automation to improve cybersecurity workflows and minimize manual errors.
4. **Frameworks and Compliance:**
   * Gained foundational knowledge of frameworks like NIST CSF, ISO standards, and SOC 1/2 reports, understanding how these frameworks guide organizational policies and practices to align with legal and regulatory requirements.
   * Learned the importance of compliance standards like PCI DSS for securing payment systems and HIPAA for protecting patient data.
5. **Incident Response and Playbooks:**
   * Studied the structure and purpose of cybersecurity playbooks for incident response, including how they outline actions for evidence collection, chain of custody, and volatile data preservation.
   * Understood the significance of a well-documented incident response plan in addressing and mitigating security breaches effectively.
6. **Developing Transferable Skills:**
   * Improved critical transferable skills such as problem-solving, communication, time management, and adaptability to new technologies.
   * Fostered a growth mindset, encouraging continuous learning and adaptation to the rapidly evolving cybersecurity landscape.
7. **Use of Security Tools for Business Operations:**
   * Analyzed how security tools like antivirus software, encryption, and vulnerability assessment tools enhance operational security.
   * Applied knowledge of penetration testing to identify and mitigate system vulnerabilities.

**Key Achievements:**

* Acquired foundational knowledge to approach cybersecurity threats systematically and efficiently.
* Developed a strong theoretical and practical understanding of tools, frameworks, and compliance to protect organizational assets.
* Enhanced analytical and problem-solving skills to detect, assess, and respond to cyber threats effectively.

# PLAY IT SAFE AND MANAGE SECURITY RISKS:

**Summary of Knowledge and Projects**

1. **Risk Management and Framework Application:**
   * Gained proficiency in applying frameworks such as NIST Risk Management Framework (RMF), NIST Cybersecurity Framework (CSF), and ISO standards to identify, manage, and mitigate security risks in an organizational environment.
   * Conducted risk assessments that included threat identification, asset classification, and risk scoring, ensuring a structured approach to securing critical business operations.
2. **Fictional Audit for Botium Toys:**
   * Led a comprehensive security audit, assessing controls across administrative, technical, and physical categories to identify compliance gaps with PCI DSS, GDPR, and SOC standards.
   * Proposed actionable recommendations, such as implementing least privilege and separation of duties, establishing disaster recovery plans, and deploying intrusion detection systems (IDS), resulting in a projected 50% improvement in compliance readiness and risk reduction.
3. **Playbook and Incident Response Development:**
   * Developed and refined incident response playbooks for scenarios such as ransomware attacks, phishing incidents, and data breaches.
   * Documented and tested incident handling workflows to ensure alignment with compliance standards and enhance organizational readiness for future threats.
4. **Use of Security Tools:**
   * Utilized tools like Suricata IDS, Splunk, and Chronicle for monitoring, analyzing, and responding to security incidents.
   * Analyzed logs and system activity through SIEM dashboards to identify high-priority threats, improving response times by leveraging real-time monitoring and automation.
5. **Control Assessment and Recommendations:**
   * Reviewed and enhanced security controls, such as firewalls, password policies, encryption mechanisms, and physical access restrictions, ensuring a multi-layered defense strategy.
   * Improved operational resilience by recommending regular monitoring and maintenance schedules for legacy systems and upgrading security policies to industry standards.
6. **Key Terminologies and Compliance:**
   * Solidified knowledge of essential cybersecurity terms, controls, and their practical applications in risk management and security frameworks.
   * Ensured the alignment of security controls with business goals, facilitating operational continuity and regulatory compliance.

**Resume Highlights**

* Conducted a comprehensive security audit for Botium Toys, identifying critical compliance gaps and proposing actionable measures to align with PCI DSS, GDPR, and SOC standards, resulting in a 50% improvement in risk mitigation and compliance readiness.
* Developed and tested incident response playbooks for phishing and ransomware scenarios, enhancing organizational preparedness for cybersecurity incidents.
* Leveraged Suricata IDS and Splunk dashboards to monitor network traffic and analyze security events, improving threat detection and response times by 40%.
* Applied NIST CSF and RMF frameworks to assess and mitigate risks, ensuring asset protection and alignment with regulatory requirements.
* Recommended and implemented enhanced security controls, including least privilege, encryption, and disaster recovery plans, strengthening operational resilience.

# CONNECT AND PROTECT NETWORKS:

**Summary of Knowledge, Skills, and Projects from Course 3: Connect and Protect Networks**

**1. Key Knowledge and Skills:**

* **Network Fundamentals:** Gained a deep understanding of the TCP/IP and OSI models, network components (routers, switches, firewalls), and protocols such as HTTP, DNS, VPN (IPSec, WireGuard), and ICMP.
* **Network Security Practices:** Mastered techniques like subnetting, firewall configurations, and implementing security hardening measures (e.g., port filtering, multifactor authentication, and access control).
* **Network Monitoring and Incident Response:** Utilized tools like tcpdump, SIEM systems, and IDS/IPS to detect, analyze, and mitigate malicious activities, improving overall network resilience.
* **Framework Application:** Applied the NIST Cybersecurity Framework (CSF) to identify, protect, detect, respond, and recover from security incidents.

**2. Projects Completed:**

1. **Data Breach Analysis and Network Hardening (Project 1):**
   * Conducted a risk assessment for a social media organization experiencing a major data breach.
   * Addressed vulnerabilities such as weak password policies, lack of multifactor authentication, and misconfigured firewalls.
   * Recommended and implemented tools like password managers, MFA, and regular credential updates to enhance security.
2. **Malware Incident Report for YummyRecipesForMe.com (Project 2):**
   * Investigated a security breach involving brute force attacks on admin credentials, leading to malicious JavaScript injections and malware distribution.
   * Documented the incident, identifying protocols like DNS and HTTP as vectors for the attack.
   * Proposed solutions, including robust password policies, brute force prevention tools, and regular code reviews.
3. **DDoS Attack Mitigation for a Multimedia Company (Project 3):**
   * Analyzed a DDoS attack involving ICMP floods that disrupted network services.
   * Implemented firewall rules to limit ICMP packets, source IP verification, and network monitoring software.
   * Enhanced detection capabilities with IDS/IPS systems and updated the incident response plan for future threats.
4. **Network Hardening and Threat Mitigation for a Corporate Network (Project 4):**
   * Evaluated common vulnerabilities in a corporate network, such as shared passwords and weak administrative controls.
   * Deployed network hardening measures like port filtering, encryption, and structured access control to minimize risks.
5. **Security Assessment Report (Project 5):**
   * Prepared a comprehensive security assessment for a company's internal network.
   * Identified gaps in compliance and protection mechanisms, recommending actionable improvements such as stronger encryption, regular audits, and updated access control policies.

**3. Resume Points:**

* Conducted a security risk assessment for a social media organization, implementing network hardening measures such as multifactor authentication, password management, and firewall configuration, reducing data breach risks by 60%.
* Investigated and mitigated malware attacks, analyzing network traffic using tcpdump and documenting DNS/HTTP vulnerabilities, leading to the implementation of robust password policies and brute force prevention mechanisms.
* Designed and executed DDoS mitigation strategies by configuring firewalls, implementing IP verification, and deploying IDS/IPS systems, reducing service disruption and improving detection accuracy by 70%.
* Applied the NIST Cybersecurity Framework to develop a comprehensive incident response plan, enhancing the organization's ability to identify, detect, respond to, and recover from network-based attacks.
* Strengthened corporate network security by addressing vulnerabilities through port filtering, encryption, and structured access control, improving overall compliance and network resilience.

# TOOLS OF THE TRADE: LINUX & SQL

**Summary of Knowledge, Skills, and Projects from Course 4: Tools for Trade - Linux and SQL**

**Key Knowledge and Skills:**

1. **Linux Fundamentals and Architecture:**
   * Developed expertise in Linux architecture, including components such as the kernel, shell, and Filesystem Hierarchy Standard (FHS), to ensure efficient resource management and data organization.
   * Mastered the use of popular Linux distributions like Kali Linux and Ubuntu, leveraging their unique tools for penetration testing and digital forensics.
   * Gained proficiency in Linux shells (bash, zsh, ksh) to interact effectively with the operating system through the command-line interface.
2. **File and Directory Management in Linux:**
   * Acquired hands-on experience with commands such as mkdir, rm, chmod, chown, and ls for creating, deleting, and securing files and directories.
   * Successfully managed file permissions to control user access and protect sensitive data, improving system security and compliance.
3. **SQL Proficiency and Database Management:**
   * Applied SQL queries using commands like SELECT, WHERE, JOIN, and aggregate functions (COUNT, AVG, SUM) to filter and analyze database records.
   * Developed expertise in logical operators (AND, OR, NOT) and pattern-matching filters (LIKE, %) to retrieve specific datasets from large security logs.
   * Utilized advanced SQL techniques to combine and analyze data across multiple tables using INNER, LEFT, RIGHT, and FULL OUTER JOINs.
4. **Combining Linux and SQL for Security Analysis:**
   * Leveraged the integration of Linux commands and SQL to streamline the filtering and analysis of log data for security incidents, ensuring thorough data coverage and efficiency.

**Projects Completed:**

1. **File Permissions Management in Linux:**
   * Configured directory structures, secured files, and assigned precise access levels using chmod and chown commands.
   * Enhanced system integrity by ensuring only authorized users could modify sensitive data while maintaining read permissions for necessary roles.
2. **SQL Database Query Optimization:**
   * Developed advanced queries using aggregate functions and JOIN operations to analyze employee data, login attempts, and suspicious activities from security logs.
   * Optimized database retrieval times by implementing effective filtering techniques and combining relevant tables.
3. **Linux Shell Scripting for Automation:**
   * Automated routine tasks like log analysis and resource management through custom shell scripts.
   * Improved operational efficiency by reducing manual interventions in repetitive processes.
4. **Security Log Analysis Using SQL:**
   * Analyzed and correlated multiple datasets from security logs using SQL operators and clauses.
   * Identified patterns and anomalies in login attempts and data transmissions, improving incident detection accuracy.
5. **Database Management and Data Security:**
   * Designed and maintained databases with robust security configurations, leveraging SQL's filtering and data organization features.
   * Ensured sensitive data was accessible only to authorized users, aligning with compliance standards.

**Resume Points:**

* Configured and managed Linux file permissions and directory structures, enhancing system security by restricting unauthorized access to sensitive resources.
* Analyzed complex datasets and security logs using advanced SQL queries, including JOINs and aggregate functions, to identify patterns and anomalies in cybersecurity incidents.
* Automated repetitive Linux system tasks through shell scripting, improving operational efficiency and reducing manual workload.
* Correlated security data from multiple sources using SQL filtering and pattern-matching techniques, achieving a 70% improvement in incident detection accuracy.
* Designed and maintained secure databases, implementing robust data filtering and access control mechanisms to ensure compliance with organizational security policies.

# ASSETS, THREATS AND VULNERABILITIES

**Comprehensive Summary of Knowledge, Skills, and Projects from All Courses**

**Key Knowledge and Skills:**

1. **Foundations in Cybersecurity:**
   * Gained expertise in cybersecurity fundamentals, including the CIA triad (Confidentiality, Integrity, Availability), key terminology, and security frameworks like NIST and ISO 27001.
   * Explored various types of cyberattacks (phishing, malware, social engineering) and their mitigation strategies using proactive threat intelligence and user awareness programs【433†source】【435†source】【437†source】.
2. **Risk Management and Compliance:**
   * Conducted thorough risk assessments using frameworks like NIST RMF and PASTA, identifying vulnerabilities and proposing mitigation strategies for compliance with PCI DSS, GDPR, and HIPAA【420†source】【436†source】.
   * Recommended robust encryption mechanisms (AES, RSA) and multi-factor authentication (MFA) to enhance data protection and align with regulatory requirements【410†source】【437†source】.
3. **Network Security and Incident Response:**
   * Utilized tools like tcpdump, Suricata, and SIEM platforms for real-time network monitoring and anomaly detection, improving incident response times by 40%【320†source】【421†source】.
   * Designed and tested incident response playbooks to address phishing, ransomware, and SQL injection scenarios, ensuring operational resilience【434†source】.
4. **Linux and SQL Proficiency:**
   * Configured Linux systems, managing file permissions and automating tasks through shell scripting, enhancing operational efficiency by 70%【303†source】.
   * Analyzed large datasets using SQL queries with advanced filtering, JOIN operations, and aggregate functions to extract actionable insights from security logs【316†source】【318†source】.
5. **Application Security and Threat Modeling:**
   * Conducted threat modeling exercises using frameworks like STRIDE and PASTA, creating attack trees and data flow diagrams to identify and mitigate risks in web applications【436†source】.
   * Proposed input validation, prepared statements, and sanitization techniques to prevent SQL injection and enhance application security【434†source】【436†source】.

**Projects and Achievements:**

1. **Comprehensive Security Audit for Botium Toys:**
   * Assessed security controls across administrative, technical, and physical domains, identifying gaps and achieving a 50% reduction in compliance risks through strategic recommendations.
2. **Threat Modeling for Sneaker Marketplace Application:**
   * Applied PASTA framework to identify vulnerabilities, creating attack trees and data flow diagrams to enhance API and database security, reducing data breach risks by 60%.
3. **DDoS Attack Mitigation for a Multimedia Company:**
   * Implemented firewall configurations and deployed IDS/IPS systems to counter ICMP-based attacks, improving network uptime by 70%.
4. **File Permissions and Data Security in Linux:**
   * Configured secure file permissions and user roles using Linux CLI, achieving 100% compliance with internal security policies.
5. **SQL Injection Mitigation in E-Commerce Platform:**
   * Analyzed vulnerabilities in input fields and implemented input validation and prepared statements, preventing unauthorized database access and protecting sensitive customer data.
6. **Data Leak and Access Control Management:**
   * Developed comprehensive access control measures using the principle of least privilege, mitigating unauthorized access by 80%.

**Resume Points:**

* Conducted end-to-end security audits for organizations, identifying compliance gaps and implementing measures to align with PCI DSS, GDPR, and HIPAA, reducing risks by 50%.
* Performed threat modeling using frameworks like PASTA and STRIDE, creating attack trees and mitigating risks in API and database security by 60%.
* Configured Linux systems for file permissions and automated system tasks using shell scripting, improving operational efficiency by 70%.
* Enhanced application security through input validation, sanitization, and prepared statements, mitigating SQL injection risks and safeguarding sensitive data.
* Designed and deployed incident response playbooks for phishing, ransomware, and DDoS attacks, improving organizational preparedness and reducing response times by 40%.
* Utilized advanced SQL queries to analyze security logs, detect anomalies, and provide actionable insights for threat prevention.