CS 668A: Practical Cyber Security for Cyber Practitioners

HOMEWORK 3

Group - 5

Group Members: (All members contributed)

1. **AKASH SHIVAJI VARUDE (231110006) (Group Lead)**
2. **A ATULYA SUNDARAM (210001)**
3. **DHIRAJ PAREEK (231110012)**
4. **KOMALA YARAMAREDDY (231110024)**
5. **TANMAY RAMJANAM DUBEY (231110052)**
6. **KUNDAN GURJAR (160354)**

Assumptions about the bank:

1. Security Patch Management: Assuming that the bank has a process in place for managing security patches for its operating systems, applications, and network devices to protect against known vulnerabilities.
2. Employee Access Controls: Assuming that the bank uses access controls to restrict employee access to sensitive information and systems. This assumption ensures that access is granted based on the principle of least privilege, enhancing overall security
3. Data Backup and Recovery: Assuming that the bank regularly backs up its critical data and has a plan in place for data recovery in the event of data loss or corruption. This assumption helps ensure that the bank can recover critical data in the event of a security incident.
4. Vendor Risk Management: Assuming that the bank assesses and manages the cybersecurity risks posed by its third-party vendors, who may have access to its systems or data.
5. User Awareness Training: Assuming that the bank provides training to its employees on cybersecurity awareness, including best practices for protecting sensitive information.
6. Incident Monitoring: Assume that the bank monitors its network and systems for suspicious activity and has mechanisms in place to detect and respond to potential security incidents.
7. Online Banking : Assume that the bank has digital banking services through website and Mobile app.
8. Remote Working : Assume that the bank allows employees to work remotely.
9. ATM services : Assumethat the bank provide ATM services
10. HTTP Server running on Linux : Assume that it also runs Ubuntu 18.04

Question1: List the cyber threats you consider for your risk assessment exercise.

1. Phishing Scams: Cybercriminals may target the bank's employees and customers with phishing scams, attempting to steal sensitive information such as passwords and card details through deceptive emails or messages.

2. Network Intrusion: Attackers could try to gain unauthorized access to the bank's network by exploiting vulnerabilities in software or through weak passwords, potentially compromising sensitive data.

3. Data Theft: Cybercriminals may target sensitive customer information and financial data for theft, which could lead to financial losses and damage to the bank's reputation.

4. ATM Skimming: Criminals could install skimming devices on ATMs to capture cardholder data, enabling them to create counterfeit cards for unauthorized withdrawals.

5. Malware: Malicious software could infect the bank's systems, leading to data breaches, operational disruptions, or unauthorized access to sensitive information.

6. Ransomware Attacks: The bank's systems could be targeted by ransomware attacks, encrypting critical data and demanding a ransom for decryption, resulting in financial losses and operational disruptions.

7. Man-in-the-Middle (MITM) Attacks: Attackers could intercept and modify communications between the bank and its customers, potentially accessing sensitive information.

8. SQL Injection Attacks: Web-based applications, such as online banking portals, could be vulnerable to SQL injection attacks, allowing attackers to steal or manipulate data.

9. DDoS Attacks: Distributed Denial-of-Service (DDoS) attacks could be launched against the bank's online services, disrupting availability and causing frustration among customers.

10. Spoofing: Attackers could create deceptive websites or emails resembling the bank's, aiming to steal sensitive information from employees and customers.

11. Cyber Risk Associated with Remote Work: Remote workers accessing sensitive information may face cybersecurity risks, especially when using personal devices outside secure environments.

12. Threats From an Internal Employee: Disgruntled employees may ignore security practices or intentionally leak data, posing a significant threat to the bank's cybersecurity.

13. Fraud and Identity Theft: Evolving through digital channels, fraud and identity theft pose significant threats to bank.

14. Privacy Concerns: Unauthorized access to CCTV footage could lead to privacy violations if sensitive information about employees or customers is captured and misused.

15. Physical Security Breaches: If the CCTV network is not adequately secured, physical intruders could potentially gain access to the network and tamper with surveillance equipment or footage.

Question 2: What kind of vulnerabilities should be considered? How are you going to find the vulnerabilities?

1) **Software Vulnerabilities:** Vulnerabilities in the operating systems (Windows 11, Windows 10, Ubuntu 18.04) and applications running on the bank's machines and servers could be exploited by attackers. These vulnerabilities may arise from outdated software versions, unpatched systems, or insecure configurations.

   Even after assuming that the bank has a process in place for managing security patches for its operating systems and applications, there are several other reasons software vulnerabilities can exist:

   I. **Delay in Patch Deployment:** There is patch management process, but there can be delays in deploying patches which can leave systems vulnerable for some period of time.
   II. **Incomplete Patching:** Patching of systems can be done Not all systems may be patched promptly, leaving some systems vulnerable even if others are up to date.
   III. **Zero-Day Exploits:** New vulnerabilities, known as zero-day exploits, can be discovered by attackers before patches are available, leaving systems vulnerable.
   IV. **Third-Party Software:** Vulnerabilities in third-party software, which may not be as diligently managed as core operating systems, can still pose a risk.
   V. **Configuration Errors:** Insecure configurations, such as incorrect permissions or settings, can create vulnerabilities that are not addressed by patch management.
   VI. **Legacy Systems:** Older systems or applications that are no longer supported by vendors may not receive patches, leaving them vulnerable.
   VII. **Insufficient Testing:** Patches that are not properly tested before deployment can introduce new vulnerabilities or cause system instability.

2) **Network Vulnerabilities:** The bank's network segmentation and firewall (Fortigate 6500F) help protect against unauthorized access. However, misconfigurations or vulnerabilities in the firewall, routers, or switches could still be exploited by attackers to gain access to the bank's internal network or intercept sensitive information.

   I. **Inadequate Monitoring and Logging:** Without proper monitoring and logging of network traffic, the bank may not be able to detect suspicious activity or potential attacks in a timely manner, which can allow attackers to remain undetected.
   II. **Denial of Service (DoS) Attacks:** Attackers could launch DoS attacks against the bank's network devices, such as routers or firewalls, to disrupt network operations and potentially gain unauthorized access during the chaos.

3) Authentication Vulnerabilities (biometric): While biometric authentication adds a layer of security, vulnerabilities such as weak biometric systems or bypass methods could compromise authentication mechanisms, allowing unauthorized access to bank systems.

I. **Biometric System Vulnerabilities:** If the biometric data is not securely stored or encrypted, it could be intercepted and used to authenticate unauthorized access attempts.
II. **Weaknesses in Biometric Sensors:** The biometric sensors themselves could have vulnerabilities that allow them to be spoofed or tricked. For example, certain types of fingerprint sensors may be susceptible to spoofing with fake fingerprints.
III. **Inadequate Implementation:** The implementation of the biometric authentication system could be insecure, leading to vulnerabilities. e.g, if the system does not properly verify the biometric data against stored templates, it could be susceptible to replay attacks.
IV. **Insufficient Biometric Authorization Checks:** Even if the biometric authentication is secure, there could be vulnerabilities in the authorization process that allow authenticated users to access unauthorized resources. For example, if the system does not properly check permissions, authenticated users could access sensitive information or perform unauthorized actions.

4) Access Control Vulnerabilities: Segregation of network segments based on access privileges is crucial. However, misconfiguration or weak access controls could lead to unauthorized access, especially if employees are granted more access than necessary for their roles.

I. **Misconfigured Firewall Rules:** Incorrectly configured firewall rules could allow unauthorized access between network segments. For example, a misconfiguration could allow access from the generic internet access segment to the highly privileged network segment.
II. **Weak Access Controls:** insufficient access controls could lead to employees having more access than necessary for their roles. For example, if a clerical staff member is granted access to the highly privileged network segment, it could lead to unauthorized access and potential security breaches.
III. **Unrestricted Access Between Segments:** Lack of proper access restrictions between network segments could allow unauthorized lateral movement within the network. For example, if there are no controls in place to prevent access from the low-privileged network segment to the highly privileged network segment, it could lead to unauthorized access to sensitive data or systems.
IV. **Insufficient Authentication Mechanisms:** Weak authentication mechanisms could lead to unauthorized access. For example, if the authentication process for accessing the highly privileged network segment is not secure, attackers could exploit this weakness to gain unauthorized access.

V. **Inadequate Monitoring:** Lack of monitoring and logging of access attempts could make it difficult to detect unauthorized access. For example, if there are no logs of access attempts to the highly privileged network segment, it could delay the detection of unauthorized access.

5) Social Engineering Vulnerabilities: Employees may still be susceptible to social engineering attacks, such as phishing, despite security awareness training. Attackers could exploit human vulnerabilities to gain unauthorized access or steal sensitive information.

I. **Phishing:** Due to the small size of the organization, phishing attacks could be more targeted and convincing, as attackers may tailor emails to appear more personalized and relevant to specific employees or departments. For example, an email posing as an internal memo from management could trick employees into disclosing sensitive information or clicking on malicious links.
II. **Attackers could exploit the hierarchical structure of the bank** to impersonate higher-level employees or authority figures, using pretexting to manipulate lower-level employees into providing access to sensitive information or systems.
III. **Baiting:** Since the bank operates critical servers facing the Internet, attackers could strategically place bait, such as a USB drive labeled "Employee Payslip Information," in an attempt to infect systems with malware or gain unauthorized access.

To find these vulnerabilities, a comprehensive approach should be taken:

1. **For finding software vulnerability:**
   a) **Vulnerability Scanning:** We can use reputable vulnerability scanners such as Nessus, OpenVAS, or Qualys to scan the systems for known vulnerabilities. Also we can schedule regular scans to ensure that new vulnerabilities are identified promptly. Prioritise vulnerabilities based on severity to address high-risk issues first.
   b) **Patch Management:** Establishing a patch management team responsible for overseeing the process for identifying, testing, and deploying patches. Use patch management tool for automating patch deployment. Also we need to ensure that tool can scan for vulnerabilities, download patches, and deploy them across the network. We can integrate that tool with existing systems for streamlined patching operations. Regularly review patch compliance reports to identify non-compliant systems and address issues promptly.
   c) **Penetration Testing:** Penetration testing can help us to identify vulnerabilities in the operating systems, applications, and network infrastructure used by the bank. This includes vulnerabilities such as outdated software versions, misconfigurations, and insecure coding practices that could be exploited by attackers to gain unauthorised access or disrupt bank operations. By conducting penetration tests, the bank can proactively identify and mitigate these vulnerabilities, thereby enhancing its overall security posture.

d) **Third-Party Security Assessments:** As there can be vulnerabilities in third party software, we need to ask third-party security firms to conduct security assessments and audits of the network and systems. Ensure that third-party assessments cover all critical systems and applications and provide actionable recommendations for mitigating vulnerabilities.
e) **Code review:** As we have assumed that the bank has mobile applications, code review can help identify vulnerabilities specific to mobile platforms, such as insecure data storage or inadequate authentication mechanisms. Regulatory requirements, such as the Payment Card Industry Data Security Standard (PCI DSS) or the General Data Protection Regulation (GDPR), may require our bank to conduct code reviews to check for vulnerability.

2. For Finding Network Vulnerabilities:

a) **Firewall Rule Review:** Review the firewall rules configured on the Fortigate 6500F firewall to ensure that they are configured correctly and do not expose the network to unnecessary risks. Look for overly permissive rules or rules that allow traffic from untrusted sources.
b) **Router and Switch Configuration Audit:** Conduct a configuration audit of the routers and switches used in the bank's network. Look for misconfigurations that could allow unauthorised access or compromise network security.
c) **Security Policy Review:** Review the bank's network security policies and procedures to ensure they are comprehensive and up to date. We have to ensure that policies cover aspects such as access control, data encryption, and incident response.

3. For Finding Authentication Vulnerabilities:

a) **Security Assessment of Biometric System:** We can conduct a security assessment of the biometric authentication system. This assessment would include a review of the system architecture, implementation details, and security controls. We can look for vulnerabilities such as insecure storage of biometric data, weak encryption, or lack of proper authentication mechanisms.
b) **Security Audit of Biometric Sensors:** We can conduct a security audit of the biometric sensors used by the bank including the assessment of the sensor's security features, resistance to spoofing, and compliance with industry standards.
c) **Biometric Data Protection Assessment:** Assess the bank's practices for protecting biometric data, including how it is stored, transmitted, and used. Look for vulnerabilities in the data protection mechanisms that could compromise the security of biometric authentication.

4. **For Finding Access Control Vulnerabilities:**

    a) **Security Audit and Review:** This security audit should include reviewing firewall rules, router configurations, and access control lists (ACLs) to identify misconfigurations or weaknesses.
    b) **Access Control Policy Review:** We can review bank's access control policies and procedures to ensure they are comprehensive and aligned with security best practices. Look for gaps or inconsistencies that could lead to unauthorized access.
    c) **Access Monitoring and Logging:** We have to implement access monitoring and logging mechanisms to track and record access attempts between network segments. Analyze the logs regularly to detect any unauthorized access attempts or anomalies.
    d) **User Access Reviews:** Conducting regular reviews of user access permissions to ensure that employees have the minimum level of access necessary for their roles. We can either remove or adjust access permissions as needed to reduce the risk of unauthorized access.

5. **For Finding Social Engineering Vulnerabilities:**

    a) **Phishing Simulations:** We can conduct phishing simulation campaigns to test employees' susceptibility to phishing attacks. These simulations can help identify employees who may require additional security awareness training.
    b) **Incident Response Exercises:** We can conduct incident response exercises that include scenarios involving social engineering attacks. This can help identify gaps in the bank's incident response procedures and improve the organization's overall security posture.

Question 3: Explain your rationale for the likelihood of various threat, vulnerability combinations. For the vulnerabilities you identify and threats you consider, build a matrix to show the qualitative likelihood for all the pairs (threat, vulnerability).

Threat / Vulnerability	Software Vulnerabilities	Network Vulnerabilities	Authentication Vulnerabilities (biometric)	Access Control Vulnerabilities	Social Engineering Vulnerabilities
Phishing Scams	High	Moderate	Moderate	Moderate	High
Network Intrusion	Moderate	Moderate	Low	Moderate	Low
Data Theft	High	Moderate	Low	Moderate	Low
ATM Skimming	Low	Low	Low	Moderate	Low
Malware	High	Moderate	Low	Moderate	Low
Ransomware Attacks	Moderate	Moderate	Low	Moderate	Low
Man-in-the-Middle Attacks	Low	Low	Low	Moderate	Low
SQL Injection Attacks	Low	Low	Low	Moderate	Low
DDoS Attacks	Low	Low	Low	Moderate	Low
Spoofing	Low	Low	Low	Moderate	Low
Remote Work Cyber Risks	Low	Low	Low	Moderate	Low
Internal Employee Threats	Low	Low	Low	Moderate	Low

Fraud and Identity Theft	Low	Low	Low	Moderate	Low
Privacy Concerns	Low	Low	Low	Moderate	Low
Physical Security Breaches	Low	Low	Low	Moderate	Low

Rationale:

- Phishing Scams:
  - Software Vulnerabilities: High likelihood due to potential vulnerabilities in email clients or browsers that attackers can exploit to deliver phishing emails.
  - Network Vulnerabilities: Moderate likelihood as phishing emails can bypass network security measures if not properly configured.
  - Authentication Vulnerabilities: Moderate likelihood if attackers can trick users into revealing authentication details through phishing emails.
  - Access Control Vulnerabilities: Moderate likelihood if phishing leads to unauthorised access due to compromised credentials.
  - Social Engineering Vulnerabilities: High likelihood as phishing relies on social engineering to deceive users.
- Network Intrusion:
  - Software Vulnerabilities: Moderate likelihood if attackers exploit vulnerabilities in network services or protocols.
  - Network Vulnerabilities: Moderate likelihood if there are misconfigurations or unpatched systems in the network.
  - Authentication Vulnerabilities: Low likelihood unless network devices are compromised through other means.
  - Access Control Vulnerabilities: Moderate likelihood if weak access controls allow attackers to gain network access.
  - Social Engineering Vulnerabilities: Low likelihood as network intrusion typically involves technical exploitation rather than social engineering.
- Data Theft:
  - Software Vulnerabilities: High likelihood if attackers exploit vulnerabilities to gain access to sensitive data.
  - Network Vulnerabilities: Moderate likelihood if attackers intercept data in transit due to network vulnerabilities.
  - Authentication Vulnerabilities: Low likelihood unless attackers bypass authentication mechanisms.

- ➢ Access Control Vulnerabilities: Moderate likelihood if access controls are weak and allow unauthorized access to data.
- ➢ Social Engineering Vulnerabilities: Low likelihood unless attackers use social engineering to gain access to data.

❖ ATM Skimming:

- ➢ Software Vulnerabilities: Low likelihood as ATM skimming is more related to physical security of the ATM.
- ➢ Network Vulnerabilities: Low likelihood unless attackers use network-based attacks to compromise ATMs.
- ➢ Authentication Vulnerabilities: Low likelihood unless attackers use stolen authentication credentials for accessing ATMs.
- ➢ Access Control Vulnerabilities: Moderate likelihood if physical access controls to ATMs are weak.
- ➢ Social Engineering Vulnerabilities: Low likelihood as ATM skimming is a more technical attack.

❖ Malware:

- ➢ Software Vulnerabilities: High likelihood as malware exploits vulnerabilities to infect systems.
- ➢ Network Vulnerabilities: Moderate likelihood as malware may spread through network vulnerabilities.
- ➢ Authentication Vulnerabilities: Low likelihood unless malware is used to steal authentication credentials.
- ➢ Access Control Vulnerabilities: Moderate likelihood if malware allows unauthorized access to systems.
- ➢ Social Engineering Vulnerabilities: Low likelihood unless malware is delivered through social engineering tactics.

❖ Ransomware Attacks:

- ➢ Software Vulnerabilities: High likelihood as ransomware exploits software vulnerabilities to infect systems.
- ➢ Network Vulnerabilities: Moderate likelihood as ransomware may spread through network vulnerabilities.
- ➢ Authentication Vulnerabilities: Low likelihood unless ransomware is used to steal authentication credentials.
- ➢ Access Control Vulnerabilities: Moderate likelihood if ransomware allows unauthorized access to systems.
- ➢ Social Engineering Vulnerabilities: Low likelihood unless ransomware is delivered through social engineering tactics.

❖ Man-in-the-Middle (MITM) Attacks:

- ➢ Software Vulnerabilities: Low likelihood unless attackers exploit vulnerabilities in software for MITM attacks.
- ➢ Network Vulnerabilities: High likelihood as MITM attacks rely on intercepting network traffic.
- ➢ Authentication Vulnerabilities: Low likelihood unless MITM attacks are used to steal authentication credentials.

- ➢ Access Control Vulnerabilities: Low likelihood unless MITM attacks lead to unauthorized access.
- ➢ Social Engineering Vulnerabilities: Low likelihood as MITM attacks are more technical in nature.

❖ SQL Injection Attacks:
- ➢ Software Vulnerabilities: High likelihood as SQL injection exploits vulnerabilities in web applications.
- ➢ Network Vulnerabilities: Low likelihood unless SQL injection is used to exploit network vulnerabilities.
- ➢ Authentication Vulnerabilities: Low likelihood unless SQL injection is used to steal authentication credentials.
- ➢ Access Control Vulnerabilities: Low likelihood unless SQL injection is used to bypass access controls.
- ➢ Social Engineering Vulnerabilities: Low likelihood unless SQL injection is delivered through social engineering tactics.

❖ DDoS Attacks:
- ➢ Software Vulnerabilities: Low likelihood as DDoS attacks do not typically exploit software vulnerabilities.
- ➢ Network Vulnerabilities: High likelihood as DDoS attacks target network infrastructure.
- ➢ Authentication Vulnerabilities: Low likelihood unless DDoS attacks are used to target authentication mechanisms.
- ➢ Access Control Vulnerabilities: Low likelihood unless DDoS attacks are used to bypass access controls.
- ➢ Social Engineering Vulnerabilities: Low likelihood as DDoS attacks are more about overwhelming resources than social engineering.

❖ Spoofing:
- ➢ Software Vulnerabilities: Low likelihood unless attackers exploit vulnerabilities in software for spoofing.
- ➢ Network Vulnerabilities: Moderate likelihood if spoofing is used to bypass network security measures.
- ➢ Authentication Vulnerabilities: Low likelihood unless spoofing is used to bypass authentication mechanisms.
- ➢ Access Control Vulnerabilities: Low likelihood unless spoofing is used to bypass access controls.
- ➢ Social Engineering Vulnerabilities: Low likelihood unless spoofing is delivered through social engineering tactics.

❖ Cyber Risk Associated with Remote Work:
- ➢ Software Vulnerabilities: Low likelihood unless remote work introduces vulnerabilities in software.
- ➢ Network Vulnerabilities: Low likelihood unless remote work introduces vulnerabilities in network configurations.
- ➢ Authentication Vulnerabilities: Low likelihood unless remote work introduces vulnerabilities in authentication mechanisms.

- ➢ Access Control Vulnerabilities: Low likelihood unless remote work introduces vulnerabilities in access controls.
- ➢ Social Engineering Vulnerabilities: Low likelihood unless remote work introduces vulnerabilities through social engineering attacks.

❖ Threats From an Internal Employee:
- ➢ Software Vulnerabilities: Low likelihood unless internal employees exploit software vulnerabilities.
- ➢ Network Vulnerabilities: Low likelihood unless internal employees exploit network vulnerabilities.
- ➢ Authentication Vulnerabilities: Low likelihood unless internal employees exploit authentication vulnerabilities.
- ➢ Access Control Vulnerabilities: High likelihood as internal employees may exploit weak access controls.
- ➢ Social Engineering Vulnerabilities: High likelihood as internal employees may be susceptible to social engineering attacks.

❖ Fraud and Identity Theft:
- ➢ Software Vulnerabilities: Low likelihood unless attackers exploit software vulnerabilities for fraud and identity theft.
- ➢ Network Vulnerabilities: Low likelihood unless attackers exploit network vulnerabilities for fraud and identity theft.
- ➢ Authentication Vulnerabilities: Low likelihood unless attackers exploit authentication vulnerabilities for fraud and identity theft.
- ➢ Access Control Vulnerabilities: Low likelihood unless attackers exploit access control vulnerabilities for fraud and identity theft.
- ➢ Social Engineering Vulnerabilities: Low likelihood unless attackers use social engineering for fraud and identity theft.

❖ Privacy Concerns:
- ➢ Software Vulnerabilities: Low likelihood unless attackers exploit software vulnerabilities to access CCTV footage.
- ➢ Network Vulnerabilities: Low likelihood unless attackers exploit network vulnerabilities to access CCTV footage.
- ➢ Authentication Vulnerabilities: Low likelihood unless attackers exploit authentication vulnerabilities to access CCTV footage.
- ➢ Access Control Vulnerabilities: Low likelihood unless attackers exploit access control vulnerabilities to access CCTV footage.
- ➢ Social Engineering Vulnerabilities: Low likelihood unless attackers use social engineering to access CCTV footage.

❖ Physical Security Breaches:
- ➢ Software Vulnerabilities: Low likelihood unless physical security breaches involve exploiting software vulnerabilities.
- ➢ Network Vulnerabilities: Low likelihood unless physical security breaches involve exploiting network vulnerabilities.
- ➢ Authentication Vulnerabilities: Low likelihood unless physical security breaches involve exploiting authentication vulnerabilities.

- ➢ Access Control Vulnerabilities: High likelihood if physical security breaches involve bypassing access controls.
- ➢ Social Engineering Vulnerabilities: Low likelihood unless physical security breaches involve social engineering tactics.

Question 4: What are the impacts/consequences of compromising the various assets?

1.Customer Information: Compromising customer information could lead to identity theft, financial fraud, and loss of customer trust. This could result in legal repercussions and damage to the bank's reputation.

Impact: (Brief description of all impacts is written after listing assets)

- Financial Loss
- Loss of customer trust
- Legal and Regulatory Consequences

2.Financial Data: Unauthorized access to financial data could lead to fraudulent transactions, financial losses, and regulatory penalties.

Impact:

- Financial Loss
- Legal and Regulatory Consequences

3.Network Infrastructure: Compromising the network infrastructure could lead to disruption of banking services, loss of data integrity, and unauthorized access to sensitive information.

Impact:

- Operational Disruption
- Data Manipulation
- Identity Theft

4.Servers: Compromising critical servers could lead to downtime, loss of data, and disruption of banking operations.

Impact:

- Operational Disruption
- Data Manipulation

5.ATMs: Compromising ATMs could lead to unauthorized withdrawals, financial losses, and damage to the bank's reputation.

Impact:

- Financial Loss
- Reputational Damage

6.CCTV Cameras: Compromising CCTV cameras could lead to loss of surveillance footage, which could hinder investigations into security incidents.

Impact:

- Data Manipulation

7.Employee Information: Compromising employee information could lead to identity theft, fraud, and damage to employee morale.

Impact:

- Identity Theft
- Reputational Damage

8.Online Banking Services: Compromising online banking services could lead to unauthorized access to customer accounts, financial losses, and damage to customer trust.

Impact:

- Financial Loss
- Loss of Customer Trust

9.Remote Work Infrastructure: Compromising remote work infrastructure could lead to unauthorized access to sensitive information and disruption of remote work operations.

Impact:

- Operational Disruption
- Identity Theft

10.ATM Services: Compromising ATM services could lead to unauthorized access to ATM funds, financial losses, and damage to customer trust.

Impact:

- Financial Loss
- Loss of customer trust

Brief Description of Impacts/consequences when above assets are compromised:

Financial Loss: Financial loss could directly impact the bank's ability to operate effectively in rural areas. It could lead to a decrease in financial services provided to rural communities which can hinder economic development in those regions. Additionally, financial losses could result in job cuts or reduced services for customers, further impacting the local economy.

Reputational Damage: Given the bank's focus on serving rural communities, reputational damage could be particularly severe. Loss of trust could lead to a significant decrease in customers, as rural populations rely heavily on trust and word-of-mouth recommendations. This could result in long-term damage to the bank's ability to operate effectively in these areas.

Operational Disruption: Any operational disruption could have a disproportionate impact on rural communities, where access to banking services may already be limited. Disruptions could lead to delays in accessing funds, processing transactions, or receiving financial assistance, affecting individuals and businesses relying on the bank's services.

Legal and Regulatory Consequences: Non-compliance with data protection regulations could result in fines or sanctions, impacting the bank's financial stability. Moreover, legal action from affected customers or regulatory bodies could further damage the bank's reputation and financial standing.

Identity Theft: Identity theft could have a significant impact on rural customers who may not have access to resources to recover from such incidents. It could result in financial losses for customers and damage the bank's reputation for security and trustworthiness.

Data Manipulation: Data manipulation could lead to incorrect financial reporting, affecting the bank's credibility and potentially leading to legal and financial consequences. It could also impact customer trust and loyalty, particularly in rural communities where personal relationships are important.

Loss of Customer Trust: Loss of customer trust could have a cascading effect, leading to a decrease in customer deposits, loans, and other financial services. This could hinder the bank's ability to serve rural communities effectively, impacting economic development in these areas.

Question 5: What are the cyber risk levels of various cyber assets? Are the controls described helping in lowering the risks? If not, what controls do you need to recommend reducing the risks to various assets.

The cyber assets that are are stake are:

1) Customer Information (5 Database Server)
2) Financial Data (5 Database Server)
3) Servers
4) CCTV Cameras (hosted on a separate network)
5) Employee Information (5 Database Server)
6) Online Banking Services (1 HTTP Server)
7) Remote Work Infrastructure
8) ATM Services
9) Windows Machines (10 and 11)
10) High Security Network
11) Low Security Network

The risk levels for each of the assets are:

1) Customer Information: Medium (Impact: High | Likelihood: Medium)

   Impact: Once a customer's information is leaked, this jeopardizes the customer-bank confidentiality that the bank promises. It also risks the customer to identity theft as well as risking their credentials not only with respect to the current bank but in all other services as well that the customer might me using.

   Likelihood: This is a medium likelihood event as this bank is prone to phishing scams and there are no controls present to restrict access to a high security device once a high security customer compromises his/her system via a phishing scam. Although the firewall present would probably prevent command and control and mitigate any data loss, but if there is some kind of privilege escalation then this would also be futile.

   Controls: Currently, there are no controls against Phishing Scams. Thus, if a scam is successful, it can easily compromise the customer information. However, access restrictions further reduces the likelihood of such scams compromising the bank.

   Recommendations: Training the bank staff against any such scams and also enable a high end filters across all accounts to prevent such access. Multi-factor authorization could also be introduced.

2) Financial Data: Low (Impact: High | Likelihood: Medium)

Impact: Once a customer's financial is leaked, this jeopardizes the customer-bank confidentiality that the bank promises. It also risks the customer's account. Banks are established on this fundamental trust that they will not allow any kind of tampering of financial information and tampering of financial data breaks this trust. There are massive consequences for such an occurrence.

Likelihood: As this information is protected in the database behind a security clearance of a manager as well as the bank account credentials of the customer. The database access from the internet is also via the HTTP server, which is protected behind the fortigate firewall. Also the databases are running Ubuntu 18.04, which after security updates resolves major CVEs. However, as the employees are very prone to phishing, this could again compromises the systems. However, there is some information about the customer that is required, which reduces the likelihood, but this information could be easily accessed.

Controls: This information is behind a robust firewall (fortigate) and access also requires privileged authorization. Once they gain access to the system, the data would also be behind an interface that would require customer authorisation. The servers are also using a moderately secure operating system with few kernel vulnerabilities. Also There is transaction approval present that decreases the likelihood further.

Recommendations: To make access to a customer's account more secure, multi-factor authorization is recommended both for the customer as well as the employees.

3) Servers: Low (Impact: High | Likelihood: Low)

Impact: If the servers are compromised, important information regarding the customer as well as their financial data is jeopardized. This is accounted for in points 1 and 2 (above).

Likelihood: The red team would have to gain access via the multiple layes of security including the firewall as well as escalating their privilege. Once inside, they would have to gain access to via kernel vulnerabilities, which can be easily patched via software updates.

Controls: These systems are behind a robust firewall (fortigate) and access also requires privileged authorization. The servers are also using a moderately secure operating system with fewer kernel vulnerabilities.

Recommendations: Consider subsctiption of the systems to Ubuntu Pro in order to receive updates till 2028 as this OS reached EOL in 2023.

4) CCTV Cameras: Medium (Impact: Medium | Likelihood: Low)

Impact: Compromising the security of the cameras could enable compromise the physical safety of the bank and also risks the employees to physical attacks possibly by dacoites and gangs. This could also prevent evidence collection and hinder capturing of fraudsters etc.

Likelihood: Because this network is accessed via the firewall, access to it is hindered greatly and chances of unauthorized access by unauthorized personnel decreases.

Controls: The existing firewall is sufficient control

5) Employee Information: Medium (Impact: High | Likelihood: Medium)

Same as the above, once Employee information is compromised, Financial data and customer data are capable of being leaked. Thus, controls for points 1 and 2 are present and the recommendations should be followed

6) Online Banking Services: Medium (Impact: High | Likelihood: Medium)

Impact: Online Transactions are critical to day-to-day life. If this is compromised, the bank could result in hampering the customer's day-to-day functioning resulting in a loss in customer trust and financial loss for the customer, which are crucial to any bank.

Likelihood: Because the bank used a single HTTP server making it highly susceptible to DDOS as well multiple HTTP requests flooding the server.

Controls: There are no controls present as of now

Recommendations: Increase the number of HTTP servers and distribute the service over multiple servers so as to prevent such denial-of-service attacks.

7) Remote Work Infrastructure: Low (Impact: Low | Likelihood: Medium)

Impact: This could hamper the productivity of the personnel working in the bank resulting in functioning of the bank

Likelihood: Multiple post-covid solutions enable remote working capabilities exist, however most like Anydesk are insecure. Thus, there is decent chance of any attacker attempting to access the systems. However, due to restricted access, there is little scope for escalation of the attack

Control: The robust firewall exists. There are also access restrictions across that prevent unauthorized employees from compromising the bank.

Recommendations: Use of secure alternatives and smarter remote work policies than decrease the requirement of any sort of privileged access remotely. Also use of decently secure solutions for remote work like Secure Remote Worker.

8) ATM Services: Low (Impact: Medium | Likelihood: Low)

   Impact: This is a localized attack that is requires physical access to the ATM. Even after it is accessed, the cyber risk levels as such is pretty minimal.

   Likelihood: As it requires physical access to the ATM itself, and direct access to the database can be provided via network lines.

   Recommendation: Assigning a watch guard to each the ATMs to prevent illegal access or theft of the ATM

9) Windows Machines: Medium (Impact: High | Likelihood: Medium)

   Impact: These are the machines that are used by the employees for day-to-day use. They contain confidential important regarding select transactions that the employees store for select users. Once the red team gains access to a system, there are two possible scenarios, depending upon the access:

   1) Access to more secure device (on highly secure network): This could result in privilege escalation, discovery and subsequent spread of the red team within the bank's systems.
   2) Access to less secure device (on less secure network): This would not be very impactful as the red team would gain access to only lower privilege systems

   Likelihood: The systems consist of Microsoft Windows 10 1903 on X86 and Windows 11 21h2 10.0.22000.739 on ARM64. Windows 10 1903 has 1053 vulnerabilities that allow remote code execution, privilege escalation and information leak with privilege escalation being the most prominent, which could endanger the bank. Windows 11 has 573 vulnerabilities with most being of the type code execution and privilege escalation. All these require access to the system via some connection which would be prevented by the firewall. Even if these systems are up to date, there might be a few vulnerabilities that could be exploited. These are protected via biometric authentication.

   Control: Currently the systems are protected by passwords and biometric authentication that the employees are given or have created themselves. There is also the firewall that would prevent any intrusion.

   Recommendation: Training to the employees to keep secure passwords on their devices as well as securing the biometric devices to prevent anyone from tampering

with it. Also employee authorization policies could be improved by training the employees to follow good work place practices such as not disclosing passwords and being mindful of their systems.

10) Network Services: Low (Impact: High | Likelihood: Low)

Impact: If these services are compromised, then this could cripple the productivity of the bank as well as prevent any sort transaction to the bank services. This could also lead to allowing the network to be monitored and allow the red team to gain access to valuable information, sent during the transaction.

Likelihood: The firewall in place is the fortigate 6500F network firewall, which provides consolidated advanced security in a smaller, more efficient physical footprint, and accommodates new security requirements such as extensive inspection of encrypted traffic for sophisticated malware without impacting performance. This is a highly robust firewall and expensive firewall that is capable of handling any sort of intrusion that the red team tries

Control: The bank has one of the best possible firewalls for network security. They should prevent access by other means

Recommendation: Refer to other recommendations