साइबर सुरक्षा और साइबर अपराध

भाग 1 – साइबर सुरक्षा (Cyber Security)

---

1. साइबर सुरक्षा का परिचय और महत्व

- **परिभाषा:**
  साइबर सुरक्षा का मतलब है कंप्यूटर सिस्टम, नेटवर्क, एप्लिकेशन और डेटा को अनधिकृत एक्सेस, चोरी, या नुकसान से सुरक्षित रखना।
- **महत्व:**
  - **डेटा सुरक्षा:** व्यक्तिगत और व्यवसायिक संवेदनशील डेटा को चोरी से बचाना।
  - **गोपनीयता:** यूज़र की जानकारी को बिना अनुमति एक्सेस होने से रोकना।
  - **बिज़नेस निरंतरता:** साइबर हमलों के बाद भी सेवाएँ चालू रखना।
  - **प्रतिष्ठा प्रबंधन:** डेटा लीक होने पर कंपनी की साख बचाना।
- **उदाहरण:**
  2021 में *Colonial Pipeline* पर रैनसमवेयर अटैक हुआ, जिससे अमेरिका में ईंधन की सप्लाई ठप हो गई।

---

2. साइबर सुरक्षा फ्रेमवर्क और मानक

फ्रेमवर्क साइबर जोखिम को मैनेज करने के लिए एक संरचित गाइडलाइन देते हैं।

1. **NIST Cybersecurity Framework**
   - **चरण:** पहचानना → सुरक्षा करना → पता लगाना → प्रतिक्रिया देना → पुनर्प्राप्त करना।

- **उद्देश्य:** संगठनों को साइबर जोखिम का आकलन और प्रबंधन करने में मदद।

2. **ISO/IEC 27001**
   - **फोकस:** *Information Security Management System (ISMS)*।
   - **तरीका:** PDCA (Plan-Do-Check-Act) के आधार पर निरंतर सुधार।
3. **COBIT**
   - **फोकस:** IT गवर्नेंस और कंट्रोल।
   - IT लक्ष्यों को बिज़नेस लक्ष्यों से जोड़ता है।

फ्रेमवर्क	मुख्य उद्देश्य	उपयोग क्षेत्र
NIST	जोखिम प्रबंधन	सरकार, क्रिटिकल इंफ्रास्ट्रक्चर
ISO 27001	ISMS	कॉर्पोरेट, बैंकिंग
COBIT	IT गवर्नेंस	ऑडिट, कम्प्लायंस

---

3. साइबर सुरक्षा खतरे (Threats)

खतरा = ऐसा कारण जो किसी अनचाहे घटना को जन्म दे सकता है।

- **मैलवेयर:**
  - वायरस, वर्म, ट्रोजन, स्पायवेयर।
  - *उदाहरण:* 2017 का WannaCry रैनसमवेयर 2 लाख+ कंप्यूटर को संक्रमित कर गया।
- **फ़िशिंग:**
  - नकली ईमेल/वेबसाइट से पासवर्ड चोरी।
- **रैनसमवेयर:**

- फाइलों को एन्क्रिप्ट कर फिरौती मांगना।

- **मैन-इन-द-मिडल अटैक:**
  - दो सिस्टम के बीच की कम्युनिकेशन को इंटरसेप्ट करना।

---

4. साइबर सुरक्षा कमजोरियां (Vulnerabilities)

कमजोरी = ऐसा दोष जिसे हैकर इस्तेमाल कर सके।

- **तकनीकी कमजोरियां:**
  - *बफर ओवरफ्लो* – मेमोरी ओवरराइट करना।
  - *SQL इंजेक्शन* – डेटाबेस में हानिकारक क्वेरी डालना।
- **मानव कमजोरियां:**
  - कमजोर पासवर्ड।
  - सोशल इंजीनियरिंग।

---

5. साइबर सुरक्षा नियंत्रण (Controls)

- **तकनीकी नियंत्रण:** फायरवॉल, IDS/IPS, एंटीवायरस।
- **प्रशासनिक नियंत्रण:** पॉलिसी, एक्सेस लिमिटेशन।
- **भौतिक नियंत्रण:** ताले, CCTV।
- **एन्क्रिप्शन:** AES-256, RSA आदि।

---

6. पहचान और एक्सेस प्रबंधन (IAM)

- **ऑथेंटिकेशन:** पासवर्ड, बायोमेट्रिक, MFA से पहचान सत्यापन।

- **ऑथराइजेशन:** रोल के आधार पर अनुमति।
- **प्रोविजनिंग:** अकाउंट बनाना/हटाना।

---

7. घटना प्रतिक्रिया और आपदा पुनर्प्राप्ति

- **इंसिडेंट रिस्पॉन्स:**
  तैयारी → पहचान → रोकथाम → सफाई → रिकवरी → सीखे गए सबक।
- **डिज़ास्टर रिकवरी:**
  बैकअप, फेलओवर, बिज़नेस कंटिन्युइटी प्लान।

---

8. साइबर सुरक्षा जागरूकता

- **क्यों ज़रूरी:** 80-90% हमले मानव गलती से होते हैं।
- **ट्रेनिंग:** फ़िशिंग टेस्ट, पासवर्ड वर्कशॉप।

भाग 2 – साइबर अपराध (Cyber Crime)

---

1. साइबर अपराध का परिचय

- **परिभाषा:**
  कंप्यूटर/नेटवर्क/डिवाइस का उपयोग करके किया गया अपराध।
- **प्रकार:** हैकिंग, पहचान की चोरी, साइबर बुलिंग, धोखाधड़ी।

---

2. साइबर अपराध कानून

- **भारत:** IT Act 2000।

- **अमेरिका:** CFAA।
- **यूरोप:** GDPR।

---

3. साइबर अपराध जांच

- सबूत पहचान → संग्रह → विश्लेषण → रिपोर्टिंग।
- **टूल्स:** EnCase, FTK।

---

4. साइबर अपराध रोकथाम

- पैच अपडेट, नेटवर्क मॉनिटरिंग, मजबूत पासवर्ड।

---

5. साइबर हमलों के प्रकार

- **DDoS:** सर्वर पर ट्रैफिक का बाढ़।
- **फ़िशिंग:** नकली संदेश।
- **स्पीयर फ़िशिंग:** टार्गेटेड फ़िशिंग।
- **SQL इंजेक्शन:** डेटाबेस छेड़छाड़।

---

6. साइबर आतंकवाद और युद्ध

- **साइबर आतंकवाद:** पब्लिक इंफ्रास्ट्रक्चर पर हमला।
- **साइबर युद्ध:** सरकार-प्रायोजित डिजिटल अटैक।

---

7. डिजिटल सबूत

- मेटाडेटा, IP लॉग, डिलीट की गई फाइलें।

---

8. अंतरराष्ट्रीय सहयोग

- इंटरपोल, CERT टीम।

भाग 3 – एडवांस थ्रेट्स और बचाव

---

1. एडवांस पर्सिस्टेंट थ्रेट (APT)

- लंबे समय तक चलने वाला लक्षित हमला।
- *उदाहरण:* APT29 – रूस से जुड़ा।

---

2. ज़ीरो-डे एक्सप्लॉइट

- पैच आने से पहले कमजोरी का फायदा उठाना।

---

3. साइबर सुरक्षा में AI और ML

- खतरे का पूर्वानुमान, बिहेवियर एनालिटिक्स।
- *उदाहरण:* Darktrace AI।

---

4. IoT सुरक्षा

- रिस्क: डिफॉल्ट पासवर्ड, अपडेट न होना।
- उपाय: नेटवर्क सेगमेंटेशन, स्ट्रॉन्ग ऑथेंटिकेशन।

---

5. क्लाउड सुरक्षा

- खतरे: मिसकन्फिगरेशन, अकाउंट चोरी।
- उपाय: एन्क्रिप्शन, Zero Trust।

---

6. ब्लॉकचेन और क्रिप्टो सुरक्षा

- खतरे: प्राइवेट की चोरी, एक्सचेंज हैक।
- उपाय: मल्टी-सिग वॉलेट, कोल्ड स्टोरेज।

---

7. क्वांटम कंप्यूटिंग

- खतरा: वर्तमान एन्क्रिप्शन तोड़ना।
- उपाय: पोस्ट-क्वांटम क्रिप्टोग्राफी।

---

8. उभरती तकनीकों की सुरक्षा

- **5G:** नेटवर्क स्लाइसिंग रिस्क।
- **ऑटोनॉमस वाहन:** सेंसर स्पूफिंग से बचाव।
