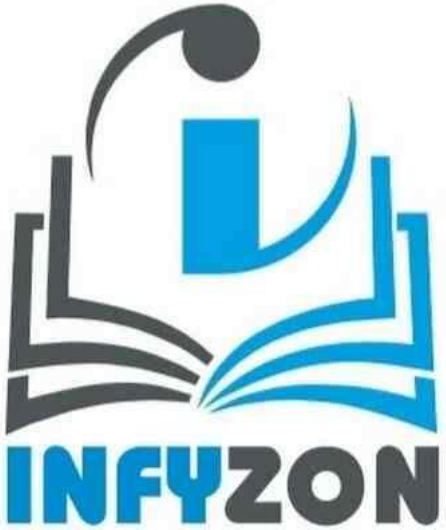


STUDY CENTER

अध्याय 14 : साइबर सुरक्षा एवं जागरूकता

परिचय :

आज आईटी **(IT – information system)** सिस्टम हमारे दैनिक जीवन के अभिन्न अंग बन गये है। ऑनलाइन लेनदेन, ऑनलाइन बैंकिग, ऑनलाइन खरिद और डेबिट कार्ड का उपयोग आधुनिक जीवन का अहम हिस्सा हैं। हम खरीदारी, शिक्षा, मनोरंजन, व्यवसाय और कई अन्य उद्देश्य के लिए कम्प्यूटर का उपयोग कर रहे है। इसलिए हमारी व्यक्तिगत जानकारी, मेडिकल रिकॉर्ड, टेक्स रिकॉर्ड, स्कूल व कॉलेज रिकॉर्ड सहित सभी प्रकार के विवरण इन कम्प्यूटरो में सेव किए जाते है।

साइबर थ्रेट के प्रकार :-

1. मैलवेयर
2. वायरस
3. ट्रोजन हॉर्स
4. स्पाइवेयर
5. फिशिंग
6. पासवर्ड हमले
7. डिनायल ऑफ सर्विसेज
8. मेलवरटाईजिंग
9. सिस्टम सिक्योरिटी में सेंध
10. वेब हमले
11. सेशन अपहरण
12. डीएनएस पोईजनिंग

1. मैलवेयर :-

मैलवेयर को आमतौर पर हानिकारक उद्देश्य वाले सॉफ्टवेयर कोड के रूप में परिभाषा किया जाता है जो कम्प्यूटर से डेटा को चोरी या नष्ट करने का प्रयास करता है। यह ईमेल अटैचमेंट और ऑपरेटिंग सिस्टम की कमजोरी के कारण कम्प्यूटर में प्रवेश करता है।

2.वायरस :-

वायरस एक नोरमल सॉफ्टवेयर प्रोग्राम होते है। जो आपके कम्प्यूटर में ई मेल अटेचमेन्ट के द्वारा भेजे जाते है फिर वो वायरस बहुत सारे वायरस को बनाता है। जो कम्प्यूटर कि वर्किंग को धीमा कर देता है।

3.ट्रोजन हॉर्स :-

ट्रोजन हॉर्स एक नुकसान नहीं पहुचाने वाला सॉफ्टवेयर प्रतित होता है लेकिन यह आपके कम्प्यूटर में वायरस या मैलवेयर को डाउनलोड करता है।

4.स्पाइवेयर :-

स्पाइवेयर एक ऐसा सॉफ्टवेयर प्रोग्राम है जो कम्प्यूटर पर आपकी गतिविधियों पर नजर रखता है। ये स्क्रिनसॉट भी लेता है।

5. फिशिंग :-

आपके ई मेल पर एक लिंक भेजा जाता हैं जिसमें क्लिक करने पर आपको अपनी व्यक्तिगत जानकारी दर्ज करने के लिए कहा जाता है। जैसे **DOB , PASSWORD , NAME , F NAME** आदि।

6. पासवर्ड हमले :-

पासवर्ड अटैक में कोई अनजान व्यक्ति आपके सिस्टम /ई–मेल खातों/ बैको के ऑनलाइन खातों तक एक एल्गोरिथ्म सॉफ्टवेयर माध्यम से पहुँचने का प्रयास करता है। जिससे आपका पासवर्ड तोडा जा सके। इससे बचने के लिए अपने पासवर्ड बड़े अक्षर छोटे अक्षर संख्या स्पेशल करेक्टर आदि का यूज करे।

7. डिनायल ऑफ सर्विसेज :-

इस हमले में हैकर डेटा को आपके कम्प्यूटर सिस्टम में भेजने के लिए कई अन्य कंम्प्यूटरों का उपयोग करता है। जो आपके कंम्प्यूटर को ऑवरलोड कर देता है और आपका कंम्प्यूटर कार्य करना बंद कर देता है। इस हमले से बचने का तरीका ये है कि अपने सिस्टम को समय समय पर अपडेट करते रहे।

8. मेलवरटाईजिंग :-

इस साइबर हमले में हमलावर एक विज्ञापन का उपयोग करता है। आप जब इन वेबसाइट पर जाते है और इन विज्ञापनों पर क्लिक करते है तो एक मैलवेयर कोड सिस्टम में डाउनलोड हो जाता है। इनसे बचना है तो व्यवहारिक ज्ञान का उपयोग करें उन विज्ञापनों पर क्लिक ना करे जो मुफ्त सामान देने का वादा करते हो।

9.सिस्टम सिक्योरिटी में सेंध :-

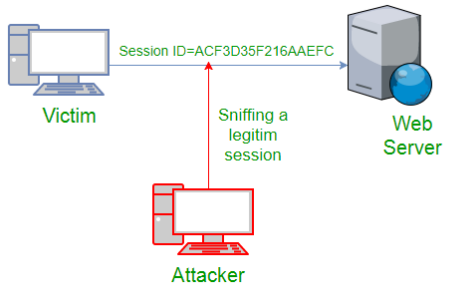
सिस्टम सिक्योरिटी में सेंध को हैकिंग या क्रैकिंग कहा जाता है इस साइबर हमले में हमलावर बिना किसी अनुमती के द्वेषपूर्ण इरादे से आपके सिस्टम में घुसपेठ करता है।

10. वेब हमले :-

अधिकांश वेबसाइट उपयोगकर्ता को वेबसाइट से बातचीत करने की सुविधा देता है। लेकिन कुछ वेबसाइट बातचीत के माध्यम से व्यक्तिगत जानकारी मांगती है।

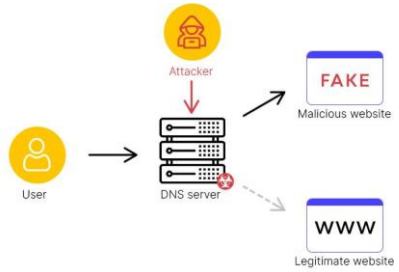
11. सेशन अपहरण :-

इस हमले में हमलावर कम्प्यूटर और सर्वर के बिच औथेन्टीकेशन सेशन की निगरानी करता है उस सेशन को अपने नियंत्रण में ले लेता है।



12. डीएनएस पोईजनिंग :-

डीएनएस पोईजनिंग में यूजर को एक वेबसाइट से दूसरी वेबसाइट पर लेजाया जाता है। जो अवैध होती है। इसमें वेबसाइड के डीएनएस पतो को बदल दिया जाता है।



❑ सुरक्षित वेबसाइटों/पोर्टलो को कैसे पहचाने :-

- स्वंय का व्यवहारीक ज्ञान व समझ आवश्यक है।
- यदि किसी वेबसाइट पर पेडलॉक नही है और **https://** नही हो तो उस वेबसाइट को न खोले।
- **https:// - Secure**
- **http:// - no Secure**
- **Website name or address** को सही से देख ले।
- बिना जानकारी वाली वेबसाइट पर किसी भी प्रकार का भुगतान न करें।

❑ सिक्योर सील :-

एक सिक्योर सील या ट्रस्ट सील वेबसाइट कंपनी पर का प्रतीक है। ट्रस्ट सील प्राप्त करने का उद्देश्य ग्राहको और साइट विजिटर्स को विश्वास दिलाना और उन्हे आश्वस्त करना है कि वेबसाइट पूरी तरह वैध और सत्यापित है। ट्रस्ट सील विभिन्न रूपो में होती है जिसमें डेटा सिक्योटी सील/बिजनेस वेरिफाइड और प्राईवेसी सील भी शामिल होती है।

❑सुरक्षित ब्राउजिंग की आदतें :-

- अपने सॉफ्टवेयर को अप-टु-डेट रखें।
- एंटी वायरस को रन करें।
- फिंशिंग हमलो से बचें।
- हर जगह एक ही पासवर्ड का यूज न करें।
- **https:** को ध्यान से चेक करें।
- गोपनीयता नीति को पढ़े **(privacy policies)**
- अपने वित्तिय लेनदेन की निगरानी रखें।
- सार्वजनिक व मुफ्त वाई फाई से बचें।
- संग्रहित पासवर्ड को अक्षम करें।
- मेलिंग शिष्टाचार।
- आईटी **(IT – information technology)** के सामाजिक/कानूनी और नैतिक पहलू को समझना।
- भारत में आईटी के लिए कानूनी ढॉचा **:-**

  भारतीय आईटी अधिनियम 2000

  धाराए – 65 / 66 / 43 / 67

THE END