इंटरनेट

यह ग्लोबल कंप्यूटर नेटवर्क है जो विभिन्न प्रकार की सूचना और संचार सुविधाएं प्रदान करता है, जिसमें स्टैंडर्डज़ेड संचार प्रोटोकॉल (टीसीपी/आईपी) का उपयोग करके परस्पर नेटवर्क शामिल हैं ।

ARPANET दुनिया का पहला पूरी तरह से परिचालन पैकेट स्विचिंग कंप्यूटर नेटवर्क था, जो 1969 में अमेरिकी रक्षा विभाग की उन्नत अनुसंधान परियोजना एजेंसी द्वारा विकसित किया गया था। यह केवल चार कंप्यूटरों से जुड़ा था। ARPANET 1983 में टीसीपी/आईपी अपनाया और "नेटवर्क के नेटवर्क" आधुनिक इंटरनेट बन गया ।

वर्ल्ड वाइड वेब - WWW इंटरनेट पर जुड़े सेवाओं में से एक है। यह इंटरनेट पर सभी जानकारी, संसाधनों, चित्रों, ध्वनियों, मल्टीमीडिया का संग्रह है जिसे एचटीएमएल में स्वरूपित किया जाता है और HTTP के माध्यम से एक्सेस किया जाता है।

वेब सर्वर - एक वेब सर्वर स्टोर, प्रक्रियाओं और उपयोगकर्ताओं के लिए वेब पृष्ठों उद्धार। हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल (HTTP) का उपयोग करके उपयोगकर्ताओं और सर्वरों के बीच अंतरसंचार किया जाता है।

वेब पेज - यह एचटीएमएल में एक दस्तावेज लिखा गया है जिसे वेब ब्राउजर का उपयोग करके इंटरनेट के माध्यम से एक्सेस किया जा सकता है। इसकी पहचान यूनिफॉर्म रिसोर्स लोकेटर द्वारा की जाती है।

वेब ब्राउज़र - यह एक सॉफ्टवेयर एप्लिकेशन है जो उपयोगकर्ताओं को वेबसाइटों तक पहुंचने की अनुमति देता है। इंटरनेट एक्सप्लोरर, गूगल क्रोम, ओपेरा, मोजिला फायरफॉक्स, यूसी ब्राउजर, एपल सफारी एक वेब ब्राउजर के कुछ उदाहरण हैं।

होम पेज - होमपेज वेबसाइट का डिफॉल्ट पेज है।

हाइपरटेक्स्ट मार्क-अप लैंग्वेज (HTML) - HTML का उपयोग इंटरनेट पर प्रदर्शित वेब पेज बनाने के लिए किया जाता है।

हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल (HTTP) - इस प्रोटोकॉल का उपयोग वेब पर डेटा स्थानांतरित करने के लिए किया जाता है। यह प्रोटोकॉल के टीसीपी/आईपी सेट के शीर्ष पर चलता है । यह एक सर्वर-क्लाइंट मॉडल का उपयोग करता है।

ट्रांसमिशन कंट्रोल प्रोटोकॉल/इंटरनेट प्रोटोकॉल (टीसीपी/आईपी)- यह संचार प्रोटोकॉल का एक सेट है जिसका उपयोग इंटरनेट तक पहुंचने के लिए किया जाता है । टीसीपी/आईपी को बॉब क्हान और विंट सेर्फ ने १९७८ में विकसित किया था ।

इंटरनेट होस्ट - होस्ट एक कंप्यूटर या एप्लिकेशन है जिसका उपयोग इंटरनेट पर डेटा स्थानांतरित करने के लिए किया जाता है। प्रत्येक होस्ट का एक अनूठा आईपी एड्रेस होता है जिसे होस्टनेम कहा जाता है।

इंटरनेट प्रोटोकॉल एड्रेस (आईपी पता) - यह एक तार्किक संख्यात्मक एड्रेस है जिसका उपयोग इंटरनेट नेटवर्क पर मेजबान की पहचान करने के लिए किया जाता है।

- आईपी का स्थिर संस्करण - आईपीवी 4 (32 बिट्स)। यह दशमलव में लिखा है और अवधि से अलग है।
- आईपी का नवीनतम संस्करण - आईपीवी 6 (128 बिट्स)। यह षोडसीमल में लिखा है और कोलोन्स द्वारा अलग किया गया है।

यूनिफॉर्म रिसोर्स लोकेटर (यूआरएल) - संसाधन और प्रोटोकॉल के पते का एड्रेस लगाने के लिए एक समान संसाधन लोकेटर (यूआरएल) का उपयोग किया जाता है।

डोमेन नाम - एक डोमेन नाम एक पते के रूप में कार्य करता है जिसका उपयोग वेबसाइट तक पहुंचने के लिए किया जाता है। इसे वेब सर्वर और ऑनलाइन संगठनों द्वारा सार्वभौमिक रूप से समझा जा सकता है।

टॉप लेवल डोमेन्स:-

डोमेन नाम	डिस्क्रिप्शन
.com	कमर्शियल
.net	नेटवर्क- ओरिएंटेड
.org	गैर-लाभकारी संगठन
.edu	पढ़ाई
.gov	सरकार
.mil	सैन्य
.int	अंतर्राष्ट्रीय संधियां

डोमेन नेम सिस्टम (डीएनएस) - डीएनएस डोमेन नामों को आईपी पतों में अनुवाद करता है। इसमें डोमेन नामों और इसके आईपी पतों का एक बड़ा डेटाबेस है।

अपलोड करना - यह कंप्यूटर से इंटरनेट सर्वर पर डेटा या फ़ाइलों के संचरण को संदर्भित करता है। अपलोड की गई फाइल किसी के द्वारा प्राप्त की जा सकती है।

डाउनलोडिंग - यह इंटरनेट से यूजर के कंप्यूटर में फाइलों की नकल करने की प्रक्रिया है।

ईमेल - इलेक्ट्रॉनिक मेल इंटरनेट पर संदेशों का संचरण है। ईमेल में, उपयोगकर्ता दस्तावेज, चित्र, वीडियो आदि संलग्न कर सकता है।

कार्बन कॉपी (CC) - इसका उपयोग एक या अधिक प्राप्तकर्ताओं के साथ ई-मेल साझा करने के लिए किया जाता है। दोनों मुख्य प्राप्तकर्ताओं और अन्य (सीसी) प्राप्तकर्ताओं सभी मेल पते देख सकते हैं।

ब्लाइंड कार्बन कॉपी (BCC) - इसमें, संदेश और अन्य प्राप्तकर्ताओं (बीसीसी) के प्राप्तकर्ता उन व्यक्तियों को नहीं देख सकते जो सभी ई-मेल प्राप्त करते हैं।

कंप्यूटर सुरक्षा

कंप्यूटर सुरक्षा भी साइबर सुरक्षा के रूप में जाना जाता है चोरी या हार्डवेयर, सॉफ्टवेयर और उन पर जानकारी के लिए नुकसान से सूचना प्रणाली की सुरक्षा है, साथ ही सेवाओं वे प्रदान की व्यवधान से ।

सुरक्षा निम्नलिखित मुद्दों पर आधारित है:

गोपनीयता: चीजों को निजी/गोपनीय रखने की क्षमता।

विश्वास: हम किसी व्यक्ति या मेजबान के डेटा पर भरोसा करते हैं।

प्रामाणिकता: आदेश में सुरक्षा साख हैं।

अखंडता: क्या प्रणाली से समझौता किया गया है/पहले से ही बदल

कंप्यूटर हैकिंग

हैकिंग कंप्यूटर सिस्टम या कंप्यूटर के अंदर निजी नेटवर्क का फायदा उठाने का प्रयास है। यह कुछ अवैध उद्देश्य के लिए कंप्यूटर नेटवर्क सुरक्षा प्रणालियों पर अनधिकृत पहुंच या नियंत्रण है ।

वायरस, कुंजी संग्रह करने वालों, रूटकिट, स्पूफिंग अटैक, पैकेट रूमाल, ट्रोजन हॉर्स और पासवर्ड क्रैकिंग हैकिंग के लिए कई तकनीकें हैं।

उनके रवैये के आधार पर हैकर्स का वर्गीकरण:

व्हाइट हैट: एक "व्हाइट टोपी" हैकर गैर दुर्भावनापूर्ण कारणों के लिए सुरक्षा टूटता है, शायद अपनी सुरक्षा प्रणाली का परीक्षण करने के लिए या जबकि एक सुरक्षा कंपनी है जो सुरक्षा सॉफ्टवेयर बनाता है के लिए काम कर रहे । शब्द "सफेद टोपी" इंटरनेट खिचड़ी भाषा में एक नैतिक हैकर को संदर्भित करता है ।

ब्लैक हैट: एक "ब्लैक हैट" हैकर एक हैकर है जो "दुर्भावना से परे या व्यक्तिगत लाभ के लिए छोटे कारण के लिए कंप्यूटर सुरक्षा का उल्लंघन करता है"। ब्लैक हैट हैकर्स डेटा को नष्ट करने, संशोधित करने या चोरी करने के लिए सुरक्षित नेटवर्क में तोड़ते हैं; या उन लोगों के लिए नेटवर्क को अनुपयोगी बनाने के लिए जो नेटवर्क का उपयोग करने के लिए अधिकृत हैं। ब्लैक हैट हैकर्स को सुरक्षा उद्योग के भीतर और आधुनिक प्रोग्रामर द्वारा "पटाखे" के रूप में भी जाना जाता है।

ग्रे हैट: एक ग्रे टोपी हैकर एक काली टोपी और एक सफेद टोपी हैकर के बीच निहित है । ग्रे हैट हैकर्स कई बार किसी सिस्टम का दोष ढूंढ लेते हैं और लोगों के ग्रुप के बजाय तथ्यों को दुनिया के सामने प्रकाशित करते हैं । हालांकि ग्रे टोपी हैकर्स जरूरी अपने निजी लाभ के लिए हैकिंग प्रदर्शन नहीं कर सकते हैं, एक प्रणाली के लिए अनधिकृत उपयोग अवैध और अनैतिक माना जा सकता है ।

ब्लू हैट: एक नीली टोपी हैकर कंप्यूटर सुरक्षा परामर्श फिल्मों के बाहर कोई है जो बग के लिए प्रयोग किया जाता है अपने प्रक्षेपण से पहले एक प्रणाली का परीक्षण, कारनामे की तलाश में तो वे बंद किया जा सकता है

नीचे दी गई श्रेणियों में से एक में वर्गीकृत थ्रेट्स:

बैक डोर्स: कंप्यूटर सिस्टम में एक पीछे का दरवाजा, एक क्रिप्टोसिस्टम सामान्य प्रमाणीकरण या सुरक्षा नियंत्रण को दरकिनार करने का कोई गुप्त तरीका है। वे मूल डिजाइन या खराब विन्यास सहित कई कारणों से मौजूद हो सकते हैं।

डिरेक्ट एक्सेस अटैक्स: कंप्यूटर तक भौतिक पहुंच प्राप्त करने वाला अनधिकृत उपयोगकर्ता सबसे अधिक संभावना है कि वह सीधे डेटा डाउनलोड कर सके।

ईवेस्ड्रोप्पिंग: यह चुपके से एक निजी बातचीत सुनने का कार्य है, आम तौर पर एक नेटवर्क पर मेजबानों के बीच ।

स्पूफिंग:उपयोगकर्ता पहचान का स्पूफिंग एक ऐसी स्थिति का वर्णन करता है जिसमें एक व्यक्ति या कार्यक्रम डेटा में हेराफेरी करके दूसरे के रूप में सफलतापूर्वक बहाना करता है।

टेम्परिंग:यह उत्पादों के दुर्भावनापूर्ण संशोधन का वर्णन करता है। तथाकथित "ईविल नौकरानी" हमलों और सुरक्षा सेवाओं राउटर में निगरानी क्षमता के रोपण

फ़िशिंग:यह उपयोगकर्ताओं से सीधे उपयोगकर्ता नाम, पासवर्ड और क्रेडिट कार्ड विवरण जैसी संवेदनशील जानकारी प्राप्त करने का प्रयास है।

वायरस के प्रकार

कंप्यूटर वायरस - एक कंप्यूटर वायरस एक दुर्भावनापूर्ण सॉफ्टवेयर प्रोग्राम है जो उपयोगकर्ता के ज्ञान के बिना उपयोगकर्ता के कंप्यूटर पर लोड होता है और दुर्भावनापूर्ण कार्रवाई करता है। स्टक्सनेट, पेट्या, रोना चाहते हैं, कोड लाल, मेलिसा, सासेर, ज़ीउस, मायडूम, क्रिप्टो लॉकर, फ्लैशबैक वायरस के कुछ उदाहरण हैं।

एल्क क्लोनर वायरस बड़े पैमाने पर फैलने वाला पहला सेल्फ-कॉपीरिंग कंप्यूटर प्रोग्राम था । इसे 1982 में 15 साल के रिच स्क्रेंटा ने बनाया था। Ryuk, Troldesh नए खोजे गए वायरस के रैंसमवेयर परिवार हैं ।

कंप्यूटर वर्म- एक कंप्यूटर कीड़ा एक दुर्भावनापूर्ण, आत्म-नकल सॉफ्टवेयर प्रोग्राम (मैलवेयर) है जो सॉफ्टवेयर और हार्डवेयर कार्यक्रमों के कार्यों को प्रभावित करता है। स्टक्सनेट सबसे प्रसिद्ध कंप्यूटर कीड़ा है।

रैंसमवेयर - रैंसमवेयर एक प्रकार का मैलवेयर प्रोग्राम है जो किसी सिस्टम को संक्रमित करता है और उस पर नियंत्रण रखता है। यह अपने मालिक से पैसे ऐंठने के इरादे से एक कंप्यूटर को संक्रमित करता है ।

बॉटनेट - बॉटनेट नेटवर्क से जुड़े कंप्यूटर/उपकरणों का एक सेट है जिसका उपयोग दुर्भावनापूर्ण उद्देश्यों के लिए किया जाता है। एक बॉटनेट में प्रत्येक कंप्यूटर को बॉट कहा जाता है। इसे ज़ोंबी के नाम से भी जाना जाता है।

ट्रोजन हॉर्स - यह एक प्रकार का मैलवेयर है जो खुद को वैध सॉफ्टवेयर के रूप में प्रस्तुत करता है। यह एक कंप्यूटर है कि वास्तविक है, लेकिन मैलवेयर कार्रवाई स्थापित करेगा पर कार्रवाई कर सकते हैं ।

कीलॉगर - एक कीलॉगर एक प्रकार का मैलवेयर है जो कंप्यूटर के सभी कीस्ट्रोक को स्टोर करता है। यह सभी प्रकार की व्यक्तिगत जानकारी, जैसे उपयोगकर्ता नाम, पासवर्ड, क्रेडिट कार्ड नंबर, और ईमेल और रिपोर्ट जैसे व्यक्तिगत दस्तावेजों को रिकॉर्ड कर सकता है।

रूटकिट - एक रूटकिट एक गुप्त कंप्यूटर प्रोग्राम है जो सक्रिय रूप से अपनी उपस्थिति छुपाते हुए कंप्यूटर तक निरंतर पहुंच प्रदान करने के लिए डिज़ाइन किया गया है। रूटकिट ट्रोजन, कीड़े, वायरस जैसे मैलवेयर से जुड़े होते हैं।

स्पाईवेयर - स्पाइवेयर एक सॉफ्टवेयर है जो अंतिम उपयोगकर्ता के ज्ञान के बिना कंप्यूटिंग डिवाइस पर स्थापित किया जाता है। यह इंटरनेट उपयोग डेटा और उपयोगकर्ता नाम और पासवर्ड जैसी संवेदनशील जानकारी चुरा रहा है, शारीरिक गतिविधि को रिकॉर्ड करने के लिए कंप्यूटर पर माइक्रोफोन या कैमरे को सक्रिय करता है।

एडवेयर - एडवेयर अवांछित सॉफ्टवेयर है जो आय उत्पन्न करने के लिए कंप्यूटर स्क्रीन पर विज्ञापन प्रदर्शित करने के लिए डिज़ाइन किया गया है। इस प्रकार के विज्ञापनों को आसानी से हटाया नहीं जा सकता है.

फ़िशिंग - फ़िशिंग एक साइबर-हमला है जो लॉगिन क्रेडेंशियल्स और क्रेडिट कार्ड नंबर सहित उपयोगकर्ता डेटा चुराने के लिए उपयोग किया जाता है। वे एक हथियार के रूप में ईमेल का उपयोग करें और विश्वास है कि संदेश बैंकों, अमेज़न आदि के रूप में असली कंपनियों से प्राप्त करने के लिए प्राप्तकर्ता के विवरण फसल में ईमेल प्राप्तकर्ता चाल । ईमेल

फ़िशिंग, भाला फ़िशिंग (लक्ष्य विशेष व्यक्ति/संगठन) फ़िशिंग की तकनीक हैं।

Smurfing - यह इनकार की सेवा हमले का एक प्रकार है कि उस नेटवर्क में आईपी पतों के हेरफेर के माध्यम से यातायात की एक बड़ी मात्रा के साथ एक नेटवर्क बाढ़ पर निर्भर करता है। इस प्रकार के हमले के परिणामस्वरूप अतिरिक्त गतिविधि की उच्च मात्रा हो सकती है, जो सर्वर या आईटी सेटअप को अभिभूत कर सकती है।

निम्नलिखित कुछ प्रसिद्ध वायरस हैं।

1. CodeRed:यह एक कीड़ा है जो माइक्रोसॉफ्ट आईआईएस सर्वर चलाने वाले कंप्यूटर को संक्रमित करता है। इस वायरस ने व्हाइट हाउस की वेबसाइट पर डॉस अटैक लॉन्च किया । यह हैकर को संक्रमित कंप्यूटर को दूर से एक्सेस करने की अनुमति देता है।

2. निंबा:यह एक कीड़ा है जो विभिन्न तरीकों का उपयोग करके खुद को फैलाता है। यह कंप्यूटर को अलग-अलग तरीकों से नुकसान पहुंचाता है।
यह फ़ाइलों को संशोधित करता है, सुरक्षा सेटिंग्स को बदलता है और प्रदर्शन को कम करता है।

3. SirCam:यह एक ईमेल लगाव के रूप में वितरित किया जाता है। यह फ़ाइलों को हटा सकता है, प्रदर्शन को नीचा दिखा सकता है और फ़ाइलों को किसी को भी भेज सकता है।

4. मेलिसा:यह एक वायरस है जिसे ईमेल अटैचमेंट के रूप में वितरित किया जाता है। यह एमएस वर्ड में विभिन्न सुरक्षा उपायों को अक्षम करता है । यह खुद को ५० लोगों को भेजता है अगर माइक्रोसॉफ्ट आउटलुक स्थापित है..

5. रिपर: यह हार्ड डिस्क से डेटा भ्रष्ट।

6. एमडीएमए: यदि दोनों फाइलें मेमोरी में हैं तो इसे एक एमएस वर्ड फ़ाइल से दूसरे में स्थानांतरित कर दिया जाता है।

7. कांसेप्ट: यह भी एक ईमेल लगाव के रूप में स्थानांतरित कर दिया है। यह अपने मूल स्थान के बजाय टेम्पलेट निर्देशिका में फ़ाइल को बचाता है।

8. वन हाफ: यह हार्ड डिस्क एन्क्रिप्ट करता है तो केवल वायरस डेटा पढ़ सकता है। एन्क्रिप्शन आधा पूरा होने पर यह स्क्रीन पर One_Half प्रदर्शित करता है