Malware

Malware

- Malware-এর পূর্ণরূপ: **Malicious Software** ম্যালওয়্যার এক ধরনের সফটওয়্যার যা তৈরি/ডিজাইন করা হয় ব্যবহারকারীর অজান্তে কোনো কম্পিউটারে অবৈধ অনুপ্রবেশ করে উক্ত কম্পিউটার সিস্টেমের ক্ষতিসাধনের উদ্দেশ্যে।

ম্যালওয়্যারের অন্তর্গত জনপ্রিয় কয়েকটি সফটওয়্যার:

- VIRUS (ভাইরাস)
- Adware (অ্যাডওয়্যার)
- Worm (ওয়ার্ম)
- Spyware (স্পাইওয়্যার)
- Trojan Horse (ট্রোজান হর্স)
- Rootkit (রুটকিট)
- Browser Hijackers
- Ransomware (র‍্যানসমওয়্যার)
- Overwrite Virus

VIRUS (ভাইরাস)

- পূর্ণরূপ: Vital Information Resources Under Seize. অর্থ: গুরুত্বপূর্ণ উৎসগুলো বাজেয়াপ্ত করা হয়েছে।
- কম্পিউটারের একটি ক্ষতিকর প্রোগ্রাম (সফটওয়্যার) যা ব্যবহারকারীর অনুমতি বা ধারণা ছাড়াই নিজে নিজেই কপি হতে পারে বা নিজের প্রতিরূপ সৃষ্টি করতে পারে।
- ভাইরাসের মূল কাজ: কম্পিউটার সিস্টেমে ঢুকে অন্য প্রোগ্রাম বা ফাইলগুলোকে মোডিফাই (modify) করে নিজের কিছু ক্ষতিকারক কোড প্রোগ্রামে লিখে দেয়।
- কম্পিউটার ভাইরাসের নামকরণ করেন: ফ্রেডরিক কোহেন। প্রথম কম্পিউটার ভাইরাস: Creeper Virus.

কম্পিউটার ভাইরাসের ক্রমভিত্তিক ইতিহাস:

সাল	তথ্যপ্রবাহ
১৯৭১	কম্পিউটার ভাইরাস আবিষ্কার করে: বব থমাস ক্রিপার।
১৯৯২	'মাইকেল অ্যাঞ্জেলা' নামক ভাইরাস কম্পিউটার সিস্টেমে প্রবেশ করে লক্ষাধিক কম্পিউটার অচল করে।
২৬ এপ্রিল ১৯৯৯	বাংলাদেশসহ বিশ্বের লক্ষাধিক কম্পিউটারে 'CIH বা চেরনোবিল' ভাইরাস প্রবেশ করে (CIH ভাইরাসের রচিয়তা: চেন ইং হাও)।
২০০৮	• 'Koobface' নামক কম্পিউটার ভাইরাস ছাড়া হয় ফেইসবুক এবং মাইস্পেসকে টার্গেট করে। • 'Conficker' নামক ভাইরাস মাইক্রোসফট সার্ভার সিস্টেমে প্রবেশ করে।
২০১৭	'শ্যাডো ব্রোকারস' নামের হ্যাকাররা 'র‍্যানসমওয়্যার' নামক এক ধরনের ম্যালওয়ার বা ভাইরাস ছড়িয়ে দেয়, যার সাহায্যে কম্পিউটারের নিয়ন্ত্রণ নিয়ে হার্ডডিস্কের অংশ বা ফাইল পাসওয়ার্ড দিয়ে অবোধ্য করে ফেলে।

কম্পিউটার সিস্টেমে ভাইরাস যেভাবে প্রবেশ করে ও প্রতিরোধের উপায়

মাধ্যম	যেভাবে প্রবেশ করে অন্য	প্রতিরোধের উপায়
মেমোরি (Memory)	অন্য কম্পিউটারে ব্যবহৃত USB Device (যেমন: Pen Drive), Hard Disk, CD, DVD ইত্যাদি নিজের কম্পিউটারে ব্যবহারের মাধ্যমে।	USB Device (যেমন: Pen Drive), Hard disk, CD, DVD ইত্যাদি থেকে ফাইল কপি করার পূর্বে Scan করতে হবে।
সফটওয়্যার (Software)	অন্য কম্পিউটার থেকে কপিকৃত সফটওয়্যার নিজের কম্পিউটারে ব্যবহারের মাধ্যমে।	অন্য কম্পিউটার থেকে কপিকৃত সফটওয়্যার ব্যবহারের আগে সফটওয়্যার ভাইরাস মুক্ত করতে হবে।
Anti-Virus	পুরাতন ভার্সনের এন্টি-ভাইরাস সফটওয়্যারের মাধ্যমে।	Update এন্টি-ভাইরাস সফটওয়্যার ব্যবহার করা।
ইন্টারনেট (Internet)	সংক্রমিত (Infected) ওয়েবসাইটের মাধ্যমে ৭০% ভাইরাস কম্পিউটার সিস্টেমে প্রবেশ করে।	ইন্টারনেট ব্যবহারের সময় Internet Security Antivirus ব্যবহার করা।
Email Attachment	ইমেইল থেকে File Attachment (যেমন: WordFile, Picture, Power Point file, Audio, Video)-এর মাধ্যমে।	সন্দেহজনক সোর্সের ই-মেইল রিসিভ না করা। যদি রিসিভ করতেই হয় তাহলে ভাইরাস মুক্ত করা।

অ্যান্টিভাইরাস (AntiVirus)

- অ্যান্টিভাইরাস: একটি Utility Software যা কম্পিউটার সিস্টেমকে ভাইরাস থেকে সার্বিক নিরাপত্তা, বিভিন্ন তথ্য, ফাইল রক্ষার জন্য প্রতিরোধক হিসেবে কাজ করে। অর্থাৎ, কম্পিউটার ভাইরাসের প্রতিষেধক প্রোগ্রামকে অ্যান্টিভাইরাস বলে।
- কাজ: বিভিন্ন ম্যালওয়্যার (যেমন: Trojan Horse, Worm, BHO (Browser Helper Object)-এর বিরুদ্ধে কাজ করে।

বর্তমানে আলোচিত ও জনপ্রিয় Anti-Virus:

- Kaspersky
- Symantec
- Virusafe
- NetQin
- Cobra
- Bitdefender
- Thunder Byte
- AVG
- E-scan
- Norton
- Panda
- Norman
- PC Cillin
- Avast
- REVE
- McAfee
- IBM Anti Virus
- Vigilant
- Avira
- Dr. Soloman toolkit

ভাইরাস ব্যতীত অন্যান্য ম্যালওয়্যার (Malware) সমূহ

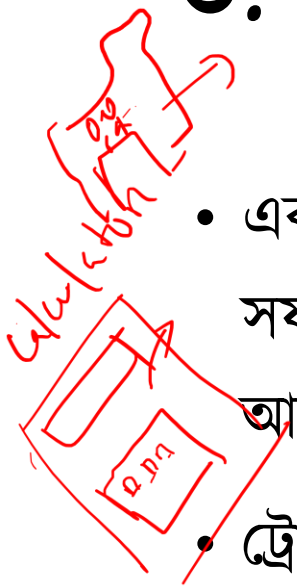
১. Worms (ওয়ার্ম)

- যে কম্পিউটার প্রোগ্রাম ইন্টারনেটের মাধ্যমে নিজে নিজেই কম্পিউটার সিস্টেমে কপি হয় তাকে ওয়ার্ম বলে।
- অপর নাম: Self-Replicating (নিজেই নিজের প্রতিরূপ তৈরি করতে পারে)। একটি স্বাধীন ম্যালওয়্যার কম্পিউটার প্রোগ্রাম যারা নিজেদের কোড এমনভাবে বদলে নেয় যে, খুঁজে বের করা কষ্টসাধ্য।
- যেভাবে কম্পিউটার সিস্টেমে প্রবেশ করে: কম্পিউটার নেটওয়ার্ক ব্যবহার করে এবং অন্য কম্পিউটারের নিরাপত্তার ব্যর্থতার সুযোগে কম্পিউটার সিস্টেমে প্রবেশ করে।
- যে ধরনের ক্ষতি করে: সবসময় নেটওয়ার্কের ক্ষতি করে, ইন্টারনেট ব্যান্ডউইথ খরচ করে।
- ওয়ার্ম এবং ভাইরাসের মধ্যকার মূল পার্থক্য: ওয়ার্ম ব্যবহারকারীর সহায়তা ছাড়াই নিজেকে ছড়িয়ে দিতে পারে, কিন্তু ভাইরাসের সচল হতে ব্যবহারকারীর স্বদিচ্ছা (নিজের ভুলে ভাইরাসকে অনুমতি দেয়া) থাকতে হয়।

২. Ransomware (র‍্যানসমওয়্যার)

- এক ধরনের ম্যালওয়্যার যা কম্পিউটার ডিভাইসকে আক্রান্ত করার পর ব্যবহারকারীকে তার মেশিনে প্রবেশ করা থেকে বিরত রাখে এবং ব্যবহারকারীর প্রবেশগম্যতা সীমাবদ্ধ করে দেয়। এই সীমাবদ্ধতা দূর করার জন্য ব্যবহারকারীর কাছ থেকে মুক্তিপণ দাবি করে।
- যেভাবে সিস্টেমে প্রবেশ করে: স্পাম/ফিশিং মেইল বা মেসেজের লিংকে প্রবেশের মাধ্যমে, সাইবার নিরাপত্তার অভাবে, দুর্বল পাসওয়ার্ডের কারণে, বিভিন্ন ওয়েব এডের মাধ্যমে।
- সবচেয়ে বেশি আক্রমণ করা র‍্যানসমওয়্যার: CryptoLocker, WannaCry (২০১৭ সালে র‍্যানসমওয়্যার দ্বারা সবচেয়ে বড় সাইবার অ্যাটাক), Crypto Wall, Locky, Petya, CryptXXX, notPetya etc.
- সবচেয়ে বেশি র‍্যানসমওয়্যার অ্যাটাক করে Windows OS এ;
- KeRanger - MacOS এ অ্যাটাক করা সাইবার অ্যাটাক।

৩. Trojan Horse (ট্রোজান হর্স) অর্থ ট্রয়ের ঘোড়া



- একটি ক্ষতিকারক কম্পিউটার প্রোগ্রাম যা কম্পিউটার সিস্টেমে সাধারণত বৈধ বা স্বাভাবিক সফটওয়্যার হিসেবে আচরণ করে এবং ব্যবহারকারীর কাছে নিজেকে অত্যন্ত কার্যকরী, সুসংবদ্ধ বা আকর্ষণীয় রূপে প্রতীয়মান করে, যাতে ব্যবহারকারী মোহিত হয়ে সফটওয়্যারটি ইন্সটল করে নেয়।
- ট্রোজান হর্স নিজের প্রতিরূপ তৈরি করতে পারে না; কিন্তু এর মাধ্যমে হ্যাকাররা কম্পিউটার সিস্টেমের নিয়ন্ত্রণ নিয়ে নেয়।
- যেভাবে কম্পিউটার সিস্টেমে প্রবেশ করে: সামাজিক প্রযুক্তি ব্যবহার করে, কোনো আকর্ষণীয় ড্রাইভ ডাউনলোড করার মাধ্যমে বা কোনো সাধারণ ফর্ম পূরণ করার মাধ্যমে।
- যে ধরনের ক্ষতি করে: কম্পিউটার সিস্টেমে ইন্টারনেট, নেটওয়ার্কের মাধ্যমে প্রবেশ করে হ্যাকাররা পারসোনাল ডেটা চুরি বা নেটওয়ার্কের পারফরম্যান্স দুর্বল করে দেয়

8. Spyware (স্পাইওয়্যার)

- ব্যবহারকারীর অজান্তে ডিভাইসে প্রবেশ করে ডিভাইসের ডেটা সংগ্রহ এবং সংগ্রহকৃত ডেটা গ্রাহকের বিনা সম্মতিতে অন্য আরেক ডিভাইসে সরবরাহ করার উদ্দেশ্যে বিশেষভাবে ডিজাইন করা একধরনের ক্ষতিকর সফটওয়্যার।
- যেভাবে প্রবেশ করে: মূলত ইন্টারনেটের মাধ্যমে। ই-মেইল, ফ্রি সফটওয়্যারের মাধ্যমে, অনিরাপদ ওয়েবসাইট থেকে ফাইল ডাউনলোড করার সময়, পপ আপ উইন্ডো এবং সোশ্যাল মিডিয়া Spam লিঙ্কের মাধ্যমে কম্পিউটারে ইন্সটল হয়।
- যে ধরনের ক্ষতি করতে পারে: আক্রান্ত ডিভাইসের যাবতীয় ইমেইল অ্যাক্টিভিটি, পাসওয়ার্ড, সোশ্যাল মিডিয়া অ্যাকাউন্ট, ক্রেডিট কার্ডের তথ্যসহ সকল তথ্য চুরি করতে পারে। অপারেটিং সিস্টেমের কনফিগারেশন পরিবর্তন করে ফেলতে পারে। এক কথায়, ব্যবহারকারীর কম্পিউটার সিস্টেমের নিয়ন্ত্রণ নিয়ে নিতে পারে।

৫. Adware (অ্যাডওয়্যার)

- এক ধরনের ক্ষতিকারক সফটওয়্যার যা ব্যবহারকারীর অনুমতি ছাড়াই অযাচিত বিজ্ঞাপন প্রদর্শন করে এবং গোপনে তথ্য সংগ্রহ করে। অ্যাডওয়্যার ব্যবহারকারীর অনিচ্ছাসত্ত্বে জোর করে অ্যাড দেখতে বাধ্য করে।
- যেভাবে সিস্টেমে প্রবেশ করে: ইন্টারনেট থেকে নিরাপত্তাহীন ওয়েবসাইটে কিছু ফাইল popup ডাউনলোড করার মাধ্যমে।
- যে কারণে ব্যবহার করা হয়: পপ-আপ অ্যাড ও স্পাম ছড়ানোর লক্ষ্যে অ্যাডওয়্যার ছড়ানো হয়।
- অ্যাডওয়্যার ব্রাউজারের মাধ্যমে অতিরিক্ত বিজ্ঞাপন দেখায়। সেজন্য এটি অন্যান্য ম্যালওয়্যারের মতো এতোটা ক্ষতিকর নয়।

৬. Rootkit (রুটকিট)

- এক ধরনের ম্যালওয়্যার যা হ্যাকারদের টার্গেট ডিভাইসে অ্যাক্সেস এবং নিয়ন্ত্রণ করার জন্য ডিজাইন করা হয়েছে।
- যেভাবে কম্পিউটার সিস্টেমে প্রবেশ করে: ফিশিং বা social engineering attack, অপারেটিং সিস্টেমের মাধ্যমে।
- অপারেটিং সিস্টেমের মাধ্যমে কম্পিউটার সিস্টেমে প্রবেশে করে এমনভাবে লুকিয়ে থাকে যে অ্যান্টিভাইরাস দ্বারা সহজে শনাক্ত করা যায় না। রুটকিট দ্বারা সফটওয়্যার, অপারেটিং সিস্টেম, হার্ডওয়্যার, ফার্মওয়্যার ক্ষতিগ্রস্ত হয় এবং হ্যাকাররা কম্পিউটার ব্যবহাকারীর পারসোনাল ইনফরমেশন জানতে পারে এবং নজরও রাখতে পারে।
- একবার কম্পিউটার সিস্টেমে প্রবেশ করতে পারলে যেকোনো ধরনের ম্যালওয়্যার ইনস্টল করতে পারে, DDoS (Distributed Denial of Service) attacks করতে পারে।

৭. Browser Hijacking (ব্রাউজার হাইজ্যাকিং)

- এক ধরনের ম্যালওয়্যার যা ব্যবহারকারীর অনুমতি ব্যতীত ব্যবহারকারীর ব্রাউজারে অযাচিত বিজ্ঞাপন দেওয়ার জন্য কোনো ওয়েব ব্রাউজারের সেটিংসকে পরিবর্তিত করে। একটি ব্রাউজার হাইজ্যাকার বিদ্যমান হোম পৃষ্ঠা, ক্রুটি পৃষ্ঠা বা সার্চ ইঞ্জিনটিতে নিজে নিজে প্রতিস্থাপন করতে পারে।
- যে কারণে ব্যবহৃত হয়: কোনো নির্দিষ্ট ওয়েবসাইটকে হিট করার জন্য ব্যবহৃত হয়, এতে করে বিজ্ঞাপনের মাধ্যমে আয় বাড়ায়।
- যেভাবে প্রবেশ করে: কম্পিউটার সিস্টেমে ইন্টারনেট থেকে 'Plugin' বা 'Extension' হিসেবে ডাউনলোড করার মাধ্যমে।
- Webpage বা Browser-এ ক্ষতিকারক popup বিজ্ঞাপন দেখায় এবং ইচ্ছার বিরুদ্ধে অন্য Website খুলে যায়।

৮. Overwrite Virus (ওভাররাইট ভাইরাস)

- সিস্টেম সংক্রমিত হওয়ার পর, ওভাররাইট ভাইরাস তার নিজস্ব কোড দ্বারা ফাইলের কনটেন্টকে ওভাররাইট করা শুরু করে। এই ভাইরাস নির্দিষ্ট ফাইল বা অ্যাপ্লিকেশনকে টার্গেট করে সংক্রমিত করতে সক্ষম। উদাহরণ: TRj.reboot
- যেভাবে কম্পিউটার সিস্টেমে প্রবেশ করে: কম্পিউটারে সিস্টেমের ফাইল এবং যেকোনো ডিলিটকৃত ফাইলের মাধ্যমে।
- ফাইল এডিট করে সিস্টেমের ক্ষতি সাধন করে, সিস্টেমের মেমোরিতে ডেটা ওভাররাইট করে মূল প্রোগ্রামের কোড ধ্বংস করে।

ফায়ারওয়াল (Firewall)

- ফায়ারওয়াল শব্দের অর্থ: নিরাপত্তা ব্যবস্থার অদৃশ্য দেয়াল।
- ফায়ারওয়াল: এক সেট নিয়ম-নীতি বা Rules যা অনুসরণ করে এবং হার্ডওয়্যার ও সফটওয়্যারের মিলিত প্রয়াসে কম্পিউটার সিস্টেমকে বাইরের আক্রমণ থেকে রক্ষা করে। অর্থাৎ, ফায়ারওয়াল হার্ডওয়্যার বা সফটওয়্যার উভয়ই হতে পারে।
- সিস্টেমের অভ্যন্তরীণ এবং বাহ্যিক নিরাপত্তার একটি Protection System (নিরাপত্তা ব্যবস্থা)।
- একটি ডিভাইস যা প্যাকেট ফিল্টার (Packet filters অপর নাম: Static Filtering), Proxy Filters-এর কাজে ব্যবহার করা হয়।

কার্যপ্রক্রিয়া

- বাইরের নেটওয়ার্ক থেকে প্রেরিত ডেটা পরীক্ষা-নিরীক্ষা করে যদি কাঙ্ক্ষিত গন্তব্যে যাওয়ার অনুমতি থাকে তাহলে সেটিকে যেতে দেয়, অন্যথায় ব্লক করে। অনাকাঙ্ক্ষিত এবং ক্ষতিকর যেকোনো কিছু আসলে ফায়ারওয়াল সেটিকে আসতে বাধা দেয় কিংবা ব্যবহারকারীকে সতর্ক করে।

ফায়ারওয়াল ব্যবহারের কারণ:

- অননুমোদিত (Unauthorized) রিমোট অ্যাক্সেস থেকে কম্পিউটারকে রক্ষা করে।
- অবাঞ্ছিত বিষয়বস্তুর সাথে সংযোগ স্থাপন করে Content-কে ব্লক করে।
- অনলাইন গেমিং নিরাপদ করে। নেটওয়ার্কের ডেটা প্রবাহ নিয়ন্ত্রণ করে।

- সবচেয়ে গ্রহণযোগ্য ফায়ারওয়াল: অভ্যন্তরীণ নেটওয়ার্ক ও ইন্টারনেটের মাঝে একটি কম্পিউটার বা রাউটার ব্যবহার করে সমস্ত ট্রাফিক পর্যবেক্ষণ করে বা নিয়ন্ত্রণ করে।

- প্রকারভেদ: ফায়ারওয়াল ২ প্রকার।
- ১. হার্ডওয়্যারনির্ভর ফায়ারওয়াল,
- ২ সফটওয়্যারনির্ভর ফায়ারওয়াল।

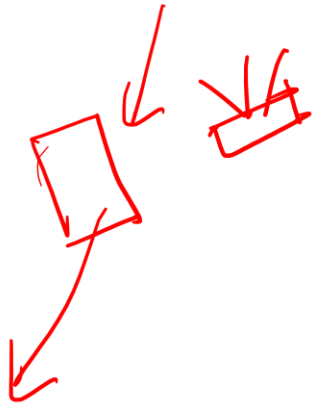
জনপ্রিয় Software Firewall:

- Norton Internet Security
- Kaspersky Internet Security
- Mcafee Internet Security
- Comodo Internet Security
- PC Tools Firewall Plus Free Edition

- ZoneAlarm Free Firewall
- Ashampoo FireWall Free
- Online Armor Free
- Agnitum Outpost Firewall Free
- Filseclab Personal Firewall Professional Edition

জনপ্রিয় Hardware Firewall:

- Cisco PIX
- Check Point
- NET screen
- WatchGuard



সাইবার অপরাধ

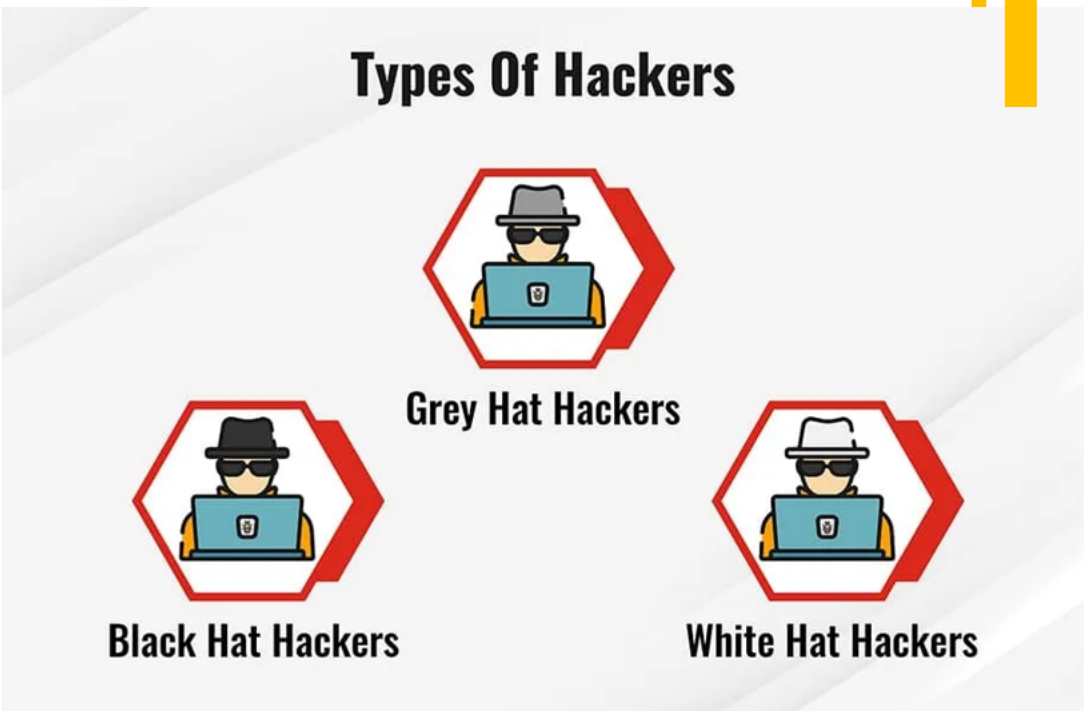
- ইন্টারনেটের মাধ্যমে যেকোনো অপরাধ (যেমন: তথ্য চুরি, তথ্য বিকৃতি, ব্ল্যাক মেইল, মানি লন্ডারিং) কে সাইবার ক্রাইম বলে।

হ্যাকিং (Hacking)

- প্রোগ্রাম রচনা ও প্রয়োগের মাধ্যমে ইন্টারনেট ব্যবহার করে অনুমতি ব্যতীত কোনো কম্পিউটার নেটওয়ার্কে প্রবেশ করে ডেটা চুরি বা ধ্বংস করে দেওয়াকে হ্যাকিং বলে।
- হ্যাকিং-এর সাথে জড়িত তাদেরকে হ্যাকার বলে।
- যারা অবৈধভাবে হ্যাকিং করে তাদেরকে ক্র্যাকার বলে।

হ্যাকার প্রধানত ৩ ধরনের-

1. হোয়াইট হ্যাট হ্যাকার: যারা অ্যাডমিনিস্ট্রেটরের অনুমতি নিয়ে সিস্টেম হ্যাক করে দুর্বলতা খুঁজে বের করে এবং তা সমাধানে সাহায্য করে। এদের কে ইথিকাল হ্যাকারও বলা হয়
2. ব্ল্যাক হ্যাট হ্যাকার: তথ্য হাতিয়ে নেয়, আর্থিক ক্ষতিসাধন করে।
3. গ্রে হ্যাট হ্যাকার: অ্যাডমিনিস্ট্রেটরের অনুমতি না নিয়ে সিস্টেম হ্যাক করে নেটওয়ার্কের দুর্বলতা খুঁজে বের করে, দুর্বল দিকগুলোকে ঠিক করার মাধ্যমে অর্থ উপার্জন করে।

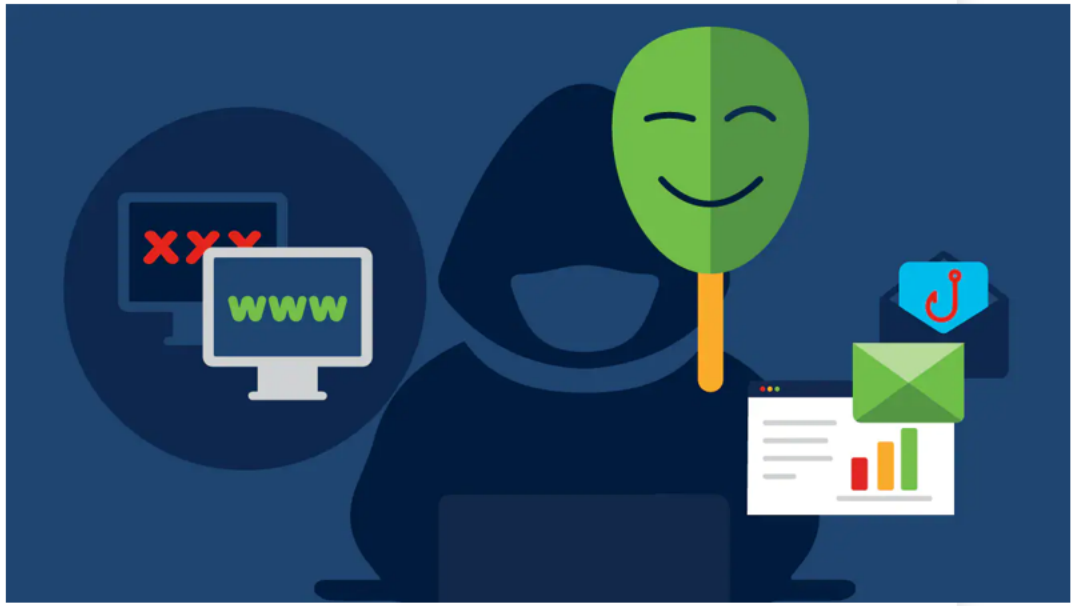


ফ্রেকিং (Phreaking)

- বিভিন্ন টেলিকমিউনিকেশন সিস্টেম হ্যাক করে অসৎ উদ্দেশ্যে ব্যবহার করার প্রক্রিয়াকে ফ্রেকিং বলে। ফোন হ্যাকারদের 'Phreaker' বলে।

স্পুফিং (Spoofing)

- ভুয়া ওয়েবসাইটের মাধ্যমে আর্থিক তথ্যাদি হাতিয়ে নেয়ার একটি সাধারণ পদ্ধতি। অসতর্ক মুহূর্তে ব্যবহারকারীরা গুরুত্বপূর্ণ ব্যক্তিগত ও আর্থিক তথ্য দিয়ে স্পুফিং-এর সাথে জড়িয়ে পড়ে।



স্নিফিং (Sniffing)

- ট্রান্সমিশন লাইন দিয়ে তথ্য যাবার সময় তথ্যকে তুলে নেয়ার একটি জনপ্রিয় পদ্ধতি। তার বা তারবিহীন ব্যবস্থাতে স্নিফিং করা হয়ে থাকে। স্নিফিং প্রতিরোধের একমাত্র উপায়: ডেটা এনক্রিপশন।

ফিশিং (Phishing)

- ইন্টারনেট ব্যবস্থায় কোন সুপ্রতিষ্ঠিত ওয়েবসাইট হুবহু নকল করে এর আদলে নতুন ওয়েবসাইট তৈরি করে কারো ব্যক্তিগত তথ্য (যেমন: User Name, Password) হাতিয়ে নেওয়াকে ফিশিং বলে।

ভিশিং (Vishing)

- মোবাইল, টেলিফোন, ইন্টারনেটভিত্তিক বিভিন্ন ফোন বা অডিও ব্যবহার করে ফিশিং করা। ফোনে লটারি বিজয়ের কথা বলে, টাকা পাঠানোর কথা বলে OTP পাঠিয়ে ব্যক্তিগত তথ্য হাতিয়ে নেওয়ার চেষ্টা করা।

সাইবারথেফট (Cybertheft)

- অসৎ উদ্দেশ্যে ব্যবহারের জন্য কিংবা অন্যান্য অবৈধ ব্যবহারের জন্য কম্পিউটার ব্যবহার করে ব্যবসায়িক অথবা ব্যক্তিগত তথ্যাদি চুরি করা।

সফটওয়্যার পাইরেসি

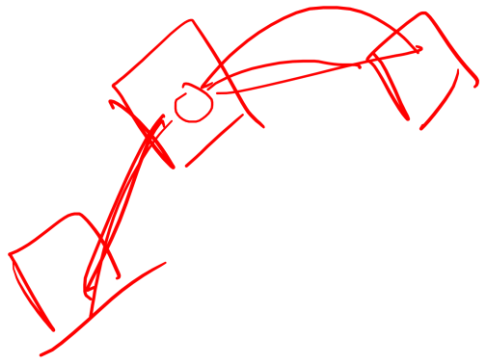
- প্রস্তুতকারীর বিনা অনুমতিতে কোনো সফটওয়্যার কপি করা, আংশিক পরিবর্তন করে নিজের নামে চালিয়ে দেয়া ইত্যাদি কার্যক্রমকে বুঝায়।

প্লেগারিজম (Plagiarism)

- কোনো ব্যক্তি বা প্রতিষ্ঠানের কোন সাহিত্য, গবেষণা বা সম্পাদনা কর্ম হুবহু নকল বা আংশিক পরিবর্তন করে নিজের নামে প্রকাশ করা। নেটভিত্তিক অন্যের তথ্যকে নিজের নামে চালিয়ে দেওয়া। সাইবার প্লেগারিজম Intellectual Property এর জন্য হুমকিস্বরূপ

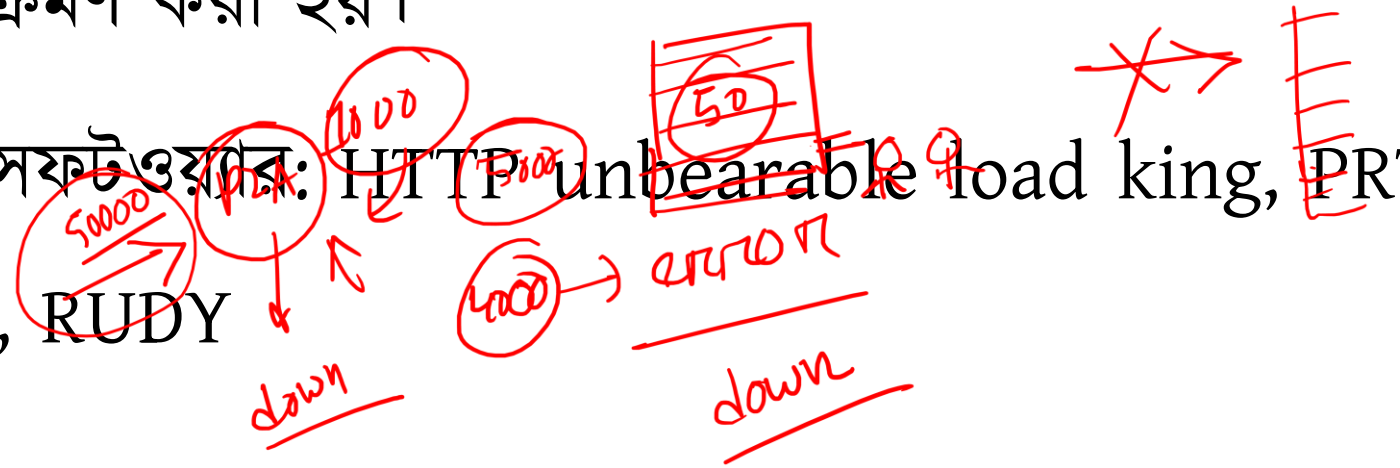
ম্যান ইন দ্য মিডল

- বিদ্যমান কথোপকথন বা ডেটা স্থানান্তরকে বাধা দেয়
- ডেটা স্থানান্তরের মাঝখানে নিজেদেরকে ঢোকানোর পরে আক্রমণকারীরা বৈধ অংশগ্রহণকারীর ভান করে।



Denial of Service (DoS) Attack

- কোনো কম্পিউটার, সিস্টেম বা ওয়েবসাইটে এই আক্রমণ সংঘটিত হলে গ্রাহকের বৈধ অনুরোধসমূহ একটি ওয়েব সার্ভার সম্পূর্ণ করতে ব্যর্থ হয়।
- কম সিকিউর ওয়েবসাইটকে কিছু সময়ের জন্য ডাউন করে ফেলার জন্য DoS আক্রমণ করা হয়।
- জনপ্রিয় সফটওয়্যার: HTTP unbearable load king, PRTG, LOIC, PyLoris, RUDY



আলোচিত হ্যাকারগোষ্ঠী

- Tailored Access Operation, NPA: USA'র সরকারি হ্যাকার।
- Cozy Bear : APT29 আইডেনটিটিধারী রাশিয়ান হ্যাকার গ্রুপ।
- কয়েকটি হ্যাকার/হ্যাকারগোষ্ঠীর নাম: তুরলা (রাশিয়ান), গ্যারি ম্যাকিনন, লুলজসিক, কেভিন পলসেন, আদ্রিয়ান লামো, জোনাথন জেমস।

কেভিন মিটনিক

- ফাদার অফ অল হ্যাকার
- যুক্তরাষ্ট্র সরকার “দেশের ইতিহাসে সেরা সাইবার ক্রিমিনাল” হিসেবে ঘোষণা দেয়

বাংলাদেশের আইনে সাইবার ক্রাইম

- In digital era, privacy must be a priority'- উক্তিটি করেছেন Al Gore.
- কম্পিউটার সিকিউরিটি দিবস- ৩০ নভেম্বর।
- ডিজিটাল বাংলাদেশ দিবস- ১২ ডিসেম্বর।
- তথ্য অধিকার আইন: ২০০৯ সালে
- ডিজিটাল নিরাপত্তা আইন: ২০১৮ সালে।
- কপিরাইট আইন: ২০০০ সালে
- তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ (সংশোধিত ২০১৩)'র আইনের ধারাসমূহ: ৫৪ ধারা, ৫৬ ধারা, ৫৭ ধারা।
- নারীদের 'সাইবার নিরাপত্তা' নিশ্চিতকরণে 'বাংলাদেশ পুলিশ'-এর উদ্যোগে চালু নতুন ইউনিট - Police Cyber Support for Women. উদ্বোধন করা হয়: ১৬ নভেম্বর, ২০২০।

Bangladesh Financial Intelligence Unit - BFIU

- বাংলাদেশের সন্দেহভাজন লেনদেন নিয়ন্ত্রণ করে। নামকরণ করা হয়: ২৫ জানুয়ারি ২০১২
- পূর্বনাম: অ্যান্টি মানিলন্ডারিং বিভাগ (চালু হয়: ২০০২ সালে)। নিয়ন্ত্রক: বাংলাদেশ ব্যাংক।
- * অর্থ পাচার ঠেকাতে 'মানিলন্ডারিং প্রতিরোধ অ্যাক্ট ২০১২' চালু হয়: ২০১২ সালে।

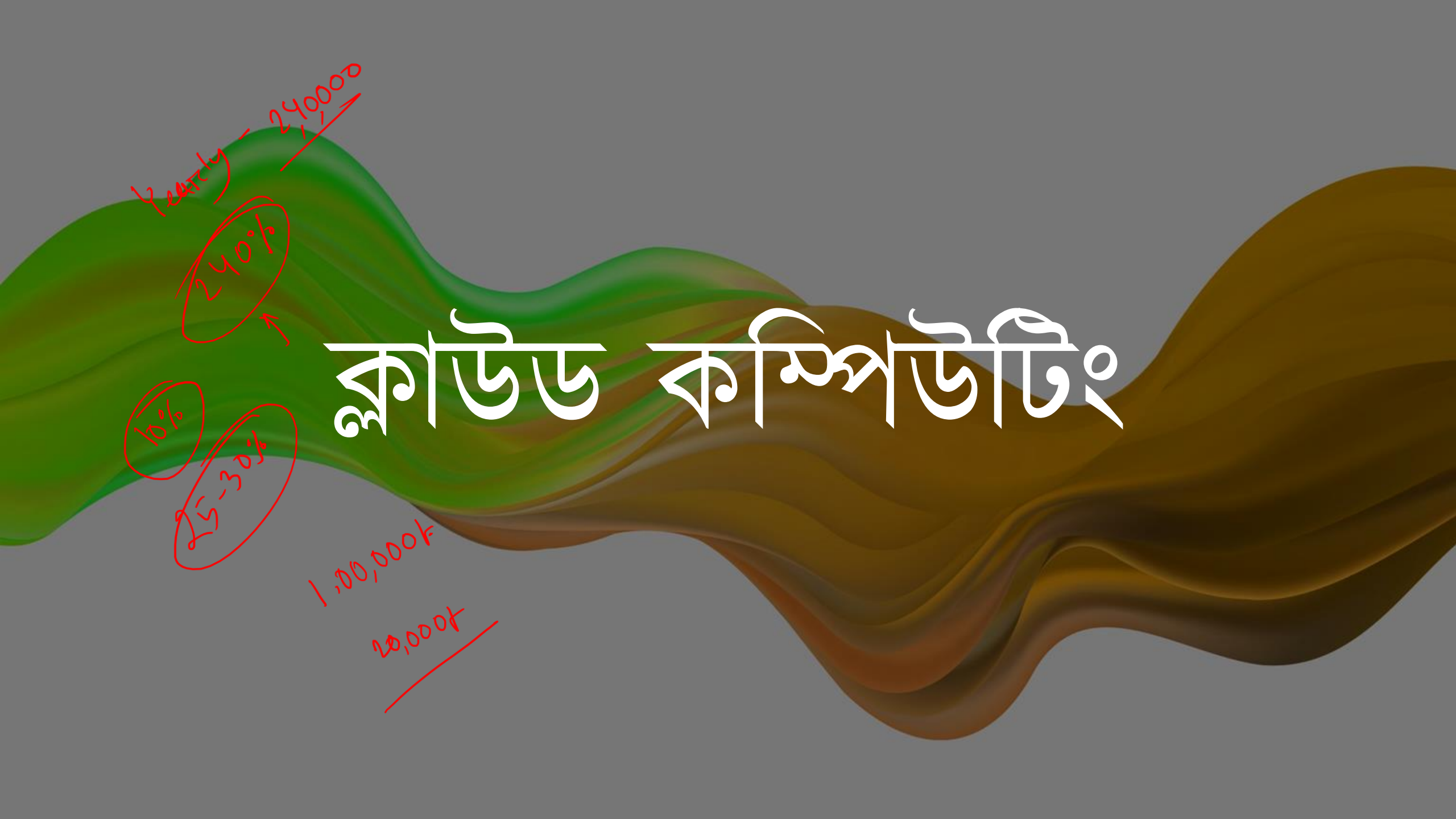
SWIFT (Society for Worldwide Interbank Financial Telecommunication)

- বিশ্বব্যাপী একটি ফান্ড ট্রান্সফার সিস্টেম এবং একটি পরিশোধন পদ্ধতি যা ব্যাংকিং সিস্টেমের সাথে সম্পর্কযুক্ত।
- সদর দপ্তর: লা হুলপে (Walloon), ব্রাসেলস, বেলজিয়াম। কোড সংখ্যা: ৮-১১টি।
- ৫ ফেব্রুয়ারি, ২০১৬ সালে যুক্তরাষ্ট্রের Federal Reserve Bank of New York থেকে সুইফট সিস্টেম ব্যবহারের মাধ্যমে বাংলাদেশ ব্যাংকের হিসাব থেকে ১০ কোটি ১০ লক্ষ ডলার (১০১ মিলিয়ন ডলার) হ্যাকিং করে ফিলিপাইনের হ্যাকাররা।

উইকিলিকস (Wikileaks) - আন্তর্জাতিক অলাভজনক প্রচার মাধ্যম

- প্রতিষ্ঠাতা: জুলিয়ান পল অ্যাসাঞ্জ (আন্তর্জাতিক হ্যাকার হিসেবে অভিযুক্ত)। প্রতিষ্ঠাকাল: ৪ অক্টোবর, ২০০৬।
- বর্তমানে উইকিলিকস বেআইনি কার্যকলাপে অভিযুক্ত।
- প্রকাশক: দ্য সানশাইন প্রেস। স্লোগান: সরকারের সব তৎপরতা হোক উন্মুক্ত। ইশতেহার: কন্সপিরেন্সি অ্যাজ গভর্ন্যান্স।
- উইকিলিকস যেভাবে আলোচনায় আসে: ২০১০ সালে বিশ্বের বিভিন্ন দেশের মার্কিন দূতাবাসগুলোর গোপন তারবার্তা, আফগানিস্তান ও ইরাক যুদ্ধে ব্যবহৃত আমেরিকার গোপন নথি ফাঁস করে আমেরিকার সামরিক গোয়েন্দা বিশ্লেষক চেলসি মেনিং (ব্রাডলি এডওয়ার্ড ম্যানিং)-এর সহযোগিতায়।

ক্লাউড কম্পিউটিং



বিগত প্রশ্ন

- অ্যামাজন এর ক্লাউড প্লাটফর্ম কোনটি? (৪৪তম) – AWS
- নিচের কোন মডেলটি Cloud Computing সেবা প্রদানকারীগণ ব্যবহার করে না? (৪৪তম) – CaaS
- নিচের কোন প্রযুক্তি 'Pay as You Go' সার্ভিস মডেল অনুসরণ করে? (৪৩তম) – Cloud Computing
- ক্লাউড কম্পিউটিং এর সার্ভিস মডেল কোনটি? (৪১তম)
- একটি প্রতিষ্ঠানে ডিভাইস ভাগাভাগি করে নেয়ার সুবিধা হলো – (৩৭তম)
- ক্লাউড সার্ভার নিচের কোনটিতে সবচেয়ে ভালো বর্ণনা করা সম্ভব – (৩৭তম) – ব্যবহারকারীর চাহিদা অনুযায়ী কম্পিউটিং সেবা দেওয়া

ক্লাউড কম্পিউটিং

- ইন্টারনেট ভিত্তিক একটি বিশেষ পরিসেবা বা ব্যবসায়িক মডেল যেখানে ক্রেতার চাহিদানুযায়ী বিভিন্ন ধরনের সেবা (যেমন: রিসোর্স শেয়ার, সার্ভার, স্টোরেজ, সফটওয়্যার প্রভৃতি) ভাড়া দেওয়া হয়।

ক্লাউড কম্পিউটিং

- ক্লাউড কম্পিউটিং সম্পর্কে মতামত দেন - জন ম্যাক ক্যার্থি।
- ক্লাউড স্টোরেজ উদ্ভাবন করেন: জোসেফ কার্ল রবনেট লিক্লাইডার।
- বাণিজ্যিকভাবে ব্যবহার শুরু করে - Amazon Web Services -(AWS); ২০০৬ সালে।

ক্লাউড কম্পিউটিং-এর বৈশিষ্ট্য - ৩টি

1. রিসোর্স স্কেলেবিলিটি
2. অন-ডিমান্ড
3. পে-অ্যাজ-ইউ-গো

ক্লাউড কম্পিউটিং-এর বৈশিষ্ট্য

১. রিসোর্স স্কেলেবিলিটি

- ক্রেতার চাহিদানুযায়ী ছোট-বড় সব ধরনের চাহিদা মেটানো হবে। ক্রেতা যতটুকু চাইবে সেবাদাতা ততটুকু পরিমাণ সেবাই দিতে পারবে।

ক্লাউড কম্পিউটিং-এর বৈশিষ্ট্য

২. অন-ডিমান্ড

- ক্রেতা যখন চাইবে তখনই সেবা দিতে পারবে। ক্রেতা তার ইচ্ছানুযায়ী চাহিদা বাড়াতে কমাতে পারবে।

ক্লাউড কম্পিউটিং-এর বৈশিষ্ট্য

৩. পে-অ্যাজ- ইউ-গো ।

- ক্রেতাকে আগে থেকে কোনো সার্ভিস রিজার্ভ করতে হবে না। ক্রেতা যা ব্যবহার করবে তার জন্যে পেমেন্ট করতে হবে।

ক্লাউড কম্পিউটিংয়ের সার্ভিস মডেল - ৩টি

১. অবকাঠামোগত সেবা (Infrastructure as a Service - IaaS)

- যেমন: ভার্চুয়াল মেশিন (CPU), ভার্চুয়াল স্টোরেজ (হার্ডড্রাইভ), নেটওয়ার্ক ভাড়া দেয়া।
- ক্লায়েন্ট-এর হাতে নিয়ন্ত্রণ থাকে। ক্ষুদ্র ব্যবসায়ীরা উপকৃত হয়।
- উদাহরণ: আমাজন ইলাস্টিক কম্পিউটিং ক্লাউড (EC2)

AWS →

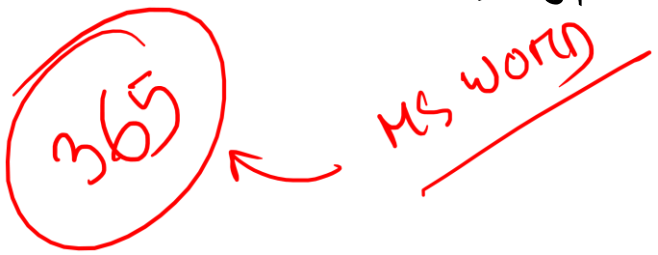
২. প্ল্যাটফর্মভিত্তিক সেবা (Platform as a Service Paas)

- অ্যাপ্লিকেশন প্রোগ্রাম, OS, ওয়েব সার্ভার, ডেটাবেজ প্রোগ্রাম তৈরি করার সুবিধা প্রদান করে।

- উদাহরণ: গুগলের অ্যাপ ইঞ্জিন।
- ক্লাউড প্রোভাইডারের নিয়ন্ত্রণ হাতে।
- সফটওয়্যার-ওয়েব ডেভেলাপার, ব্যবসায়ীরা উপকৃত হয়।

৩. সফটওয়্যার সেবা (Software as a Service - SaaS)

- ক্লাউড সেবাদানকারী প্রতিষ্ঠানের ডেভেলাপ করা অ্যাপ্লিকেশন সফটওয়্যার/প্রোগ্রাম ভাড়া দেয়।



- উদাহরণ: Google Docs দিয়ে গুগলের ক্লাউডের উপর ভিত্তি করে ইন্টারনেট ও ওয়েব ব্রাউজার ব্যবহার করে মাইক্রোসফট অফিসের (যেমন: ডকুমেন্ট, স্প্রেডশীট, প্রেজেন্টেশন) কাজ করা যায়।

ব্যবহারকারীর সংখ্যার উপর ভিত্তি করে ক্লাউড কম্পিউটিংয়ের সার্ভিস মডেল - ৪টি

- (১) পাবলিক ক্লাউড (Public Cloud)
- (২) কমিউনিটি ক্লাউড (Community Cloud)
- (৩) প্রাইভেট ক্লাইড (Private Cloud)
- (৪) হাইব্রিড ক্লাউড (Hybrid Cloud)

পাবলিক ক্লাউড (Public Cloud)

- সার্ভিসমূহ সকলের জন্য উন্মুক্ত।
- যেমন: আমাজনের EC2 সার্ভিস।
- ব্যবসার ধরন: B2C (Business to Consumer) ই-কমার্স সেবা।
- পরিচালিত হয়: সরকার, একাডেমিক বা ব্যবসায়িক সংস্থা দ্বারা।

কমিউনিটি ক্লাউড (Community Cloud)

- সার্ভিস: একটি ক্ষুদ্রতর কমিউনিটির সকলের জন্য উন্মুক্ত।
- ব্যবসার ধরন: B2C (Business to Consumer) ই-কমার্স সেবা।

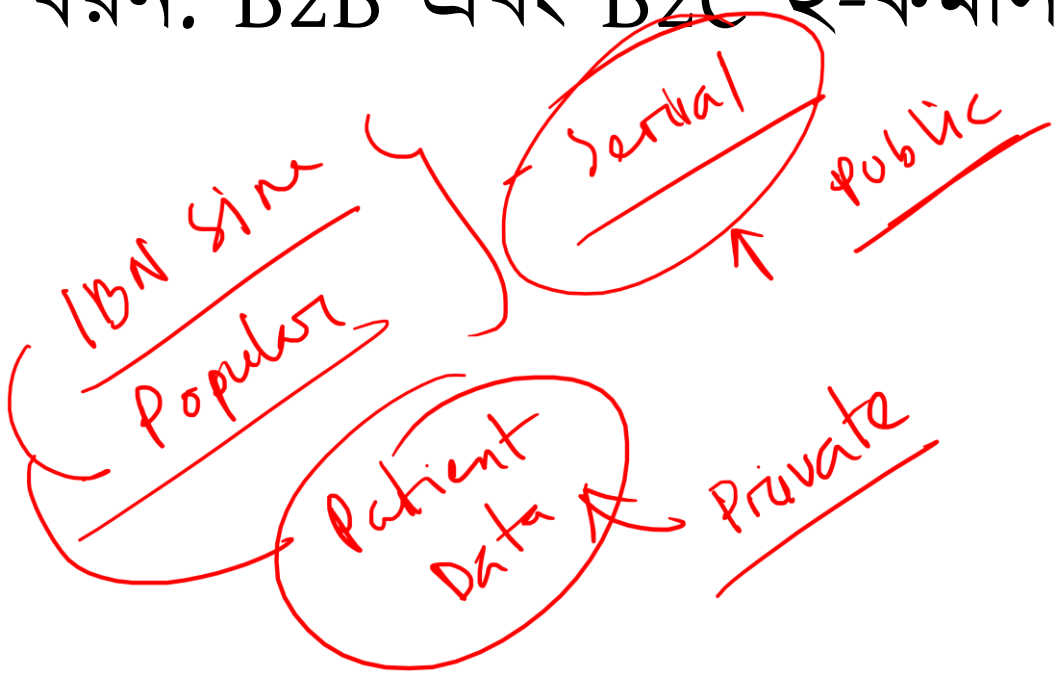
- উদাহরণ: সেনানিবাসের অফিসার-সৈনিকদের জন্য তৈরি ক্লাউড।

প্রাইভেট ক্লাইড (Private Cloud)

- একটি বড় কোনো সংস্থার নিজেদের কর্মকর্তাদের মধ্যে সীমাবদ্ধ।
- ব্যবসার ধরন: B2B ই-কমার্স সেবা।
- আন্ত-ব্যবসায়িক ক্রিয়াকলাপের জন্য বেশি ব্যবহৃত হয়।

হাইব্রিড ক্লাউড (Hybrid Cloud)

- কম্পিউটিং রিসোর্সসমূহ বিভিন্ন ক্লাউডের সাথে একত্রে আবদ্ধ।
- ব্যবসার ধরন: B2B এবং B2C ই-কমার্স সেবা।



জনপ্রিয় ক্লাউড কম্পিউটিংসমূহ

Cloud Computing	মালিকানা
Amazon Elastic Compute Cloud	Amazon
OneDrive	Microsoft
Dropbox	Dropbox
Microsoft Azure	Microsoft
iCloud	Apple
Google Drive	Google

Thank You