হ্যাকিংয়ের গোলকধাঁধা

সাইবার নিরাপত্তা নিশ্চিত করুন
ডিজিটাল বাংলাদেশ গড়ে তুলুন...

দিলোয়ার আলম
মনিরুজ্জামান সজল

উৎসর্গ

তাদেরকে,
যারা বাংলাদেশের সাইবার স্পেস নিরাপদ
রাখতে নিরলস চেষ্টা চালিয়ে যাচ্ছে।

আমাদের কথা

সময় তো সময়ের দ্বারাই নিয়ন্ত্রিত হচ্ছে। যতই দিন যাচ্ছে—আমরা প্রযুক্তির সাগরে নিমজ্জিত হচ্ছি। ইন্টারনেট পৃথিবীকে সংকুচিত করে আমাদের হাতের মুঠোয় এনে দিয়েছে। আমাদের নিত্যনৈমিত্তিক প্রায় সকল কাজই হয়ে যাচ্ছে ইন্টারনেট বা কম্পিউটার নেটওয়ার্কের ওপর নির্ভরশীল। মানবজীবনে এর সুফল যেমন আছে, কুফলও আছে ঢের। যদি যথোপযুক্ত নিরাপত্তা না দেয়া যায়, তাহলে যে কোনো সিস্টেমই হ্যাক হওয়ার সম্ভাবনা থাকে। আর সিস্টেম হ্যাকারদের হাতে চলে গেলে—কোটি কোটি টাকার লোকসান হওয়ার সম্ভাবনা তো আছেই। কী? অবাক হচ্ছেন বা গুলিয়ে ফেলছেন। ভাবছেন, কীভাবে কী করে হ্যাকাররা? আর কেনই-বা করে?

আপনি সঠিক বইটিই বাছাই করেছেন। হ্যাকিং এবং হ্যাকারদের পদযাত্রা ১৯৫০-১৯৬০ সালের দিকে শুরু হলেও আমাদের দেশে মানুষজন হ্যাকিং শব্দটির সঙ্গে পরিচিত মাত্র একযুগ ধরে। কিন্তু এই অল্পসময়ের মধ্যেই বেশ কয়েকটি সাইবারযুদ্ধে সফলতা প্রদর্শন করে বিশ্ববাসীর কাছে যথেষ্ট পরিচিতি লাভ করেছে বাংলাদেশ।

বর্তমান প্রযুক্তির যুগে আপনাকে নিরাপদ থাকতে হলে অবশ্যই সচেতন হতে হবে; জেনে নিতে হবে—নিরাপদে থাকার কৌশলগুলো। আমরা 'BugsBD Ltd'-এর পক্ষ থেকে একটি সমীক্ষা চালিয়েছিলাম—সাইবার নিরাপত্তা এবং হ্যাকিং নিয়ে। অবিশ্বাস্য হলেও সত্য যে, অধিকাংশ মানুষই সাইবার নিরাপত্তা বিষয়ে অজ্ঞ। অনেকেই জানে না—ইন্টারনেটে তাদের দেয়া বিভিন্ন তথ্য কতটুকু নিরাপদ বা আদৌ নিরাপদ কি না। কীভাবে তথ্যগুলো নিরাপদ রাখতে হবে, এই বিষয়টিও তাদের অজানা। তাই নিজেদের দায়বদ্ধতা থেকেই আমরা 'হ্যাকিংয়ের গোলকধাঁধা' বইটি প্রকাশ করার সিদ্ধান্ত নিয়েছি।

আশা রাখি, এই বইটি পড়ে পাঠক সাইবার নিরাপত্তা এবং হ্যাকিং সম্পর্কে জানতে ও ইন্টারনেটজগতে কীভাবে নিরাপদ থাকা যায় বা হ্যাকারদের ফাঁদ এড়িয়ে চলা যায় তা জানতে পারবেন।

ইতিহাস পড়তে নয়, গড়তে হবে...

কৃতজ্ঞতা স্বীকার

সাইবার সিকিউরিটি বিষয়ে গবেষণার সূচনালগ্ন থেকেই এই দুজন ব্যক্তির সমর্থন ও সাহচর্য না পেলে হয়তো আজকের এই সোনালি দিনের উদয় হতো না। তাঁরা যেভাবে আমাদের অনুপ্রেরণা ও উদ্দীপনা জুগিয়েছেন, আমাদের কর্মপ্রেরণার উৎস হিসেবে কাজ করেছেন তা ভুলবার নয়। স্যার ও ম্যাডামের কাছে চিরকৃতজ্ঞ...

মহান রাব্বুল আলামিনের কাছে তাঁদের সুস্থতা ও দীর্ঘায়ু কামনা করি।

ড. তৌহিদ ভূইয়া

প্রফেসর ও হেড
ডিপার্টমেন্ট অব সফটওয়্যার ইঞ্জিনিয়ারিং
পরিচালক
সাইবার সিকিউরিটি সেন্টার
ড্যাফোডিল ইন্টারন্যাশনাল ইউনিভার্সিটি
১০২/১ শুক্রাবাদ (মিরপুর রোড), ঢাকা-১২০৭
বাংলাদেশ।

তানজীলা ফারাহ

লেকচারার
ও
সাইবার সিকিউরিটি গবেষক
ডিপার্টমেন্ট অব ইলেকট্রিক্যাল অ্যান্ড কম্পিউটার ইঞ্জিনিয়ারিং
নর্থ সাউথ ইউনিভার্সিটি
প্লট-১৫, ব্লক-বি বসুন্ধরা, ঢাকা-১২২৯
বাংলাদেশ।

সূ চি প ত্র

অধ্যায়-১

হ্যাকিংয়ের এপিঠ-ওপিঠ

যেদিন থেকে মানুষ চাকার ব্যবহার শিখেছে, সেদিন থেকেই প্রযুক্তির উদ্ভবের যাত্রা শুরু। এই চাকাই পালটে দিয়েছে পৃথিবীর চেহারা। নিয়ে এসেছে আজকের এই চলমান আধুনিক বিশ্ব। সময়ের সঙ্গে তাল মিলিয়ে আমরাও এগোচ্ছি দারুণ ছন্দে। ইন্টারনেটের বদৌলতে ইদানীং গোটা পৃথিবী হাতে নিয়েই ঘুরছি আমরা। Facebook হোক কিংবা Skype নিজের নামের মতোই পরিচিত আমাদের কাছে। এমন কিছু নেই যা Google-এ সার্চ দিলে মেলে না।

এই আলাদিনের চেরাগের মতো জগৎ হাতে নিয়েই ঘুম থেকে উঠে দিনের যাত্রা শুরু। নিজেদের তৈরি নিয়মকানুনে নিজেকে নিয়েই সারাদিনের ব্যস্ততা শেষে রাতে যখন ঘুমাতে যাই, এই জগতের ওপরেই পুরো বিশ্বাস রেখে নিশ্চিন্তে ঘুমিয়ে পড়ি।

বিশ্বাস!

অনেক মূল্যবান একটা জিনিস। সত্যিই কী এই চেরাগ বিশ্বাসের যোগ্য? কেউ কি আপনার চেরাগকে আপনারই ক্ষতির কাজে ব্যবহার করার ক্ষমতা রাখে? ধরুন, রাতে স্বপ্নে দেখলেন—আপনার তৈরি নিয়ম ভেঙে আপনার চেরাগকে আপনার কাছ থেকে কেউ কেড়ে নিয়ে আপনারই বিপক্ষে তা ব্যবহার করছে। কী বোঝানোর চেষ্টা করছি, বুঝতে পারছেন? এই গোটা ব্যাপারটিকে আমরা তুলনা করতে পারি 'হ্যাকিং'-এর সঙ্গে। আর যারা হ্যাকিং করে তাদেরকে বলা হয় 'হ্যাকার'।

এখন বর্তমান প্রযুক্তিকে সঙ্গে নিয়ে আমরা ক্রমান্বয়ে প্রবেশ করব হ্যাকিংয়ের গোলকধাঁধায়।

১.১ গোলকধাঁধার অবতরণ ও প্রযুক্তির মগজধোলাই

এ গোলকধাঁধার প্রথম অবতরণ ১৮৭৮ সালের দিকে, একদল কিশোর যখন 'বেল টেলিফোন' নামক এক প্রতিষ্ঠানের টেলিফোন বার্তাসংযোগ বিচ্ছিন্ন ও ভুল পথে

চালিত করে নিজেদের অজান্তেই হ্যাকিং করে ফেলে। তবে ১৯৬০ সালের কম্পিউটার হ্যাকিংয়ের ঘটনাকে প্রথম স্বীকৃত কম্পিউটার হ্যাকিং হিসেবে গণ্য করা হয়। ঠিক তখন থেকেই মূলত হ্যাকিংয়ের ধারণা জনমনে দৃষ্টিগোচর হয়।

সুপ্রিয় পাঠক, এখন হয়তো নিশ্চয়ই ভাবছেন কোন কার্যক্রম বা কোন ধরনের দক্ষতাকে হ্যাকিং হিসেবে আখ্যায়িত করে যেতে পারে? এখন সেই বিষয়টিকে একটু পরিষ্কারভাবে তুলে ধরার চেষ্টা করব।

অসৎ উদ্দেশ্য সাধনের লক্ষ্যে কোনো সিস্টেমের ত্রুটিকে পুঁজি করে ঐ সিস্টেমে অনধিকার প্রবেশপূর্বক সিস্টেমের সম্পূর্ণ বা আংশিক নিয়ন্ত্রণ নিজের আয়ত্তে নেয়ার প্রক্রিয়াকেই হ্যাকিং বলে।

হ্যাকিং কোনো একটি নির্দিষ্ট কারণে সংঘটিত হয় না। অনেক ধরনের উদ্দেশ্য এটির পেছনে কাজ করে। কখনো কারও চলমান ব্যবসাকে ক্ষতিগ্রস্ত করার উদ্দেশ্যে তার সিস্টেম হ্যাক করা হয়। কখনো-বা গুরুত্বপূর্ণ তথ্য চুরি, তথ্য পরিবর্তনের জন্য কিংবা কোনো ব্যক্তি বা প্রতিষ্ঠানকে ভীতি প্রদর্শনের উদ্দেশ্যে হ্যাকিং হয়ে থাকে। প্রতিশোধ নেয়ার জন্য বা কাউকে সামাজিকভাবে হেয়প্রতিপন্ন করার জন্যও হ্যাকিং করা হয়। এ ছাড়া ধর্মীয় বা রাজনৈতিক মগজধোলাই একজন সাধারণ মানুষকে কখনো কখনো ভয়ংকর হ্যাকার হয়ে উঠতে মদদ জোগায়।

১.২ হ্যাকারদের জীবনদর্শন

একজন হ্যাকার খুবই দূরদৃষ্টিসম্পন্ন ব্যক্তি যার কম্পিউটারের ওপর স্বতন্ত্র দক্ষতা রয়েছে, যেই দক্ষতার ওপর ভিত্তি করে এবং প্রোগ্রামিং জ্ঞানের সর্বোচ্চ ব্যবহার করে সে বিভিন্ন ধরনের নতুন নতুন বিস্ময়কর স্ক্রিপ্ট, টুল ও বিভিন্ন হ্যাকিংপদ্ধতি আবিষ্কার করতে ভালোবাসে। আসলে এই ধরনের সৃজনশীলতাকে একজন হ্যাকাররা যে পর্যায়ে নিয়ে যায় তাতে একজন হ্যাকারকে বলা যেতেই পারে 'অত্যন্ত বুদ্ধিমত্তাসম্পন্ন টেকনোলজিস্ট'।

সব হ্যাকারের জীবনদর্শন একরকম নয়, মূলত জীবনদর্শনের ওপর ভিত্তি করেই তাদের চিন্তা-চেতনা, অনুধাবন ও সমস্যা সমাধানের ভিন্নতর পদ্ধতি গড়ে ওঠে। তবে হ্যাকারদের অনেক ভিন্নতার মধ্যেও একটি চরম সাদৃশ্য খুঁজে পাওয়া যায় আর সেটি হলো তার প্রত্যেকটা বিষয়ের সঙ্গে টেকনোলজির যোগসাজশ খুঁজে বের করা এবং সমস্যা থেকে উত্তরণের জন্য প্রোগ্রামিংয়ের দক্ষতা কাজে লাগানো। মূলত তাদের জেদি মনোভাবই সাধারণ মস্তিষ্কধারীদের থেকে একটু আলাদাভাবে জাত চেনাতে সাহায্য করে। দিনের পর দিন একটি সমস্যা থেকে উত্তরণের উপায় বের করার জন্য বাইরের জগতে কী হচ্ছে সেসব না ভেবে চিন্তায় মগ্ন থাকার প্রয়াসই তাকে সফলতার দিকে একধাপ এগিয়ে যেতে সাহায্য করে।

১.৩ হ্যাকারদের ধরন

দেশে যেমন অপরাধী থাকে, অপরাধী ধরার জন্য তেমনি প্রশাসনও থাকে। আসলে এই হ্যাকার তথা সাইবার অপরাধীদের ধরা বা প্রতিরোধ করা যেমন-তেমন মানুষের কাজ নয়। বিশ্বব্যাপী এমন কিছু মানুষও আছে যারা চিন্তা করে হ্যাকারের মতো, আর কাজ করে সাইবার অপরাধীদের প্রতিরোধের জন্য। এদেরকে বলা হয় এথিক্যাল হ্যাকার। এরা সাধারণত দেশের সাইবার স্পেসকে নিরাপদ রাখার জন্য কাজ করে।

এই অনুচ্ছেদে আমরা কয়েক প্রকার হ্যাকার সম্পর্কে জানব।

- **Black Hat Hacke (আনএথিক্যাল হ্যাকার) :** এই জাতীয় হ্যাকাররা নিজেদের কম্পিউটারবিজ্ঞানের বুদ্ধিমত্তাকে খারাপ কাজে লাগিয়ে তথ্য চুরি, পরিবর্তন, ফাঁস, মুক্তিপণ দাবিসহ সাইবারজগতের সব ধরনের অপরাধ করে থাকে।

- **White Hat Hacker (এথিক্যাল হ্যাকার) :** যে হ্যাকার তার হ্যাকিং দক্ষতাকে কাজে লাগিয়ে সাইবার ক্রাইম প্রতিরোধ এবং সাইবার নিরাপত্তা নিশ্চিত করার জন্য কাজ করে, তাকে White Hat Hacker বলে। এদেরকে এথিক্যাল হ্যাকার বা সিকিউরিটি অ্যানালিস্টও বলা হয়ে থাকে।

- **Grey Hat Hacker (গ্রে হ্যাট হ্যাকার) :** যেদিকে বৃষ্টি, সেদিকে ছাতা! ভালো আর খারাপের সংমিশ্রণ। এরা কখনো ব্ল্যাক হ্যাটদের মতো কাজ করে আবার মন চাইলে হোয়াইট হ্যাটদের মতোও কাজ করে।

- **Suicide Hacker:** নিশ্চিত সাজা হবে জেনেও নির্দিষ্ট উদ্দেশ্য হাসিলের জন্য এরা হ্যাক করে। ধরা পড়লে নিশ্চিত মৃত্যুদণ্ড হবে জেনেও এরা হ্যাকিং চালিয়ে যায়।

- **Script Kidie:** এরা ততটা দক্ষতাসম্পন্ন হ্যাকার নয়। সাধারণত অভিজ্ঞ হ্যাকারদের তৈরি করা টুলস ও স্ক্রিপ্ট ব্যবহার করে এরা হ্যাক করে থাকে।

- **Cyber Terrorist:** যে হ্যাকিংয়ের কারণে কোনো সমাজ বা জাতির ওপরে বড় ধরনের প্রভাব পড়ে, তাকে Cyber Terrorism বলে। এবং যে হ্যাকাররা Cyber Terrorism-এর সঙ্গে জড়িত, তাদেরকে Cyber Terrorist বলে।

- **Hacktivist:** সাধারণত রাজনৈতিক, সামাজিক, ধর্মীয় ইস্যু, মানবাধিকার বা তথ্য আন্দোলনের স্বাধীনতা সম্পর্কিত অবস্থানকে কেন্দ্র করে যে সমস্ত হ্যাকিংয়ের ঘটনা ঘটে থাকে, সেগুলোকে মূলত হ্যাকটিভিজমের আওতায় আনা যায়। হ্যাকটিভিজম ভালো অথবা খারাপ উভয় কারণে হয়ে থাকে। যদিও এটি নিয়ে মতভেদ রয়েছে। যেসব হ্যাকার হ্যাকটিভিজমের সঙ্গে জড়িত থাকে, তাদেরকে হ্যাকটিভিস্ট বলা হয়। এরা মূলত কোনো আন্দোলনের বার্তা পৌঁছে দেয়ার জন্য অ্যাকটিভিটি পরিচালনা করে থাকে।

১.৪ হ্যাকিংয়ে হাতেখড়ি

একজন হ্যাকার যখন উপলব্ধি করে কোনো ব্যক্তির বা প্রতিষ্ঠানের কোনো সিস্টেমে তার জন্য গুরুত্বপূর্ণ কিছু তথ্য রয়েছে, তখনই সে হ্যাকিংয়ে উদ্যত হয়। একটি সফল হ্যাকিং অ্যাটাকের প্রথম থেকে শেষ পর্যন্ত হ্যাকার যে ধাপগুলো অবলম্বন করে, সেসব সম্পর্কেই আমরা এখন জানব।

- **Information Gathering:** হ্যাকিংয়ের প্রথম ধাপ হিসেবে একজন হ্যাকারের প্রধান কাজ হলো তার টার্গেট সিস্টেম সম্পর্কে তথ্য সংগ্রহ করা।

  যেমন : যদি একজন হ্যাকার কোনো প্রতিষ্ঠান/কোম্পানিকে টার্গেট করে, সে ক্ষেত্রে ঐ প্রতিষ্ঠানের গ্রাহক কারা, কারা চাকরি করে, কী কী সেবা তারা সরবরাহ করে, কোন নেটওয়ার্ক ব্যবহার করে, ঐ প্রতিষ্ঠান কোন অপারেটিং সিস্টেম ব্যবহার করে—এই সাধারণ তথ্যগুলো হ্যাকার সংগ্রহ করে।

  অনেক সময় হ্যাকার প্রত্যক্ষভাবে তথ্য সংগ্রহ করে। যেমন : হেল্প ডেস্কে ফোন দিয়ে তার প্রয়োজনীয় বিভিন্ন তথ্য সে জেনে নিতে পারে। হেল্প ডেস্কে থাকা ব্যক্তিটি হয়তো মনে করবে এই তথ্য আর এমন কী! কিন্তু ঐ সাধারণ তথ্যই হ্যাকারের জন্য খুবই গুরুত্বপূর্ণ হতে পারে।

  আবার অনেক সময় প্রতিষ্ঠান/কোম্পানির বাৎসরিক তথ্য, যা সর্বসাধারণের জন্য দেয়া থাকে সেসব দেখেও হ্যাকার অনেক গুরুত্বপূর্ণ তথ্য পরোক্ষভাবে পেয়ে যেতে পারে, যা তার হ্যাকিংয়ে সহায়ক।

- **Scanning:** পূর্ববর্তী ধাপে পাওয়া তথ্যগুলোতে এবার হ্যাকার চালায় চিরুনি বিশ্লেষণ। Port Scanner, Network mapper, Ping tools ইত্যাদি সফটওয়্যার ব্যবহার করে ঐ প্রতিষ্ঠানের ব্যবহৃত নেটওয়ার্ক কাঠামো, লাইভ মেশিন, বিভিন্ন পোর্ট, পোর্টের স্ট্যাটাস, অপারেটিং সিস্টেমের বিস্তারিত তথ্য—এসব ইনফরমেশনগুলো সংগ্রহ করে ফেলে।

- **Gaining Access:** এ পর্যায়ে হ্যাকার তার টার্গেট করা সিস্টেমের ভেতরে কারও অনুমতি ছাড়াই অবৈধভাবে প্রবেশ করতে সক্ষম হয়। সিস্টেম বলতে কোম্পানি/প্রতিষ্ঠানের অপারেটিং সিস্টেম প্রতিষ্ঠান যে নেটওয়ার্কের সঙ্গে সংযুক্ত, সেই নেটওয়ার্ক লেভেল এবং অ্যাপ্লিকেশন লেভেল (সফটওয়্যার বা ওয়েবসাইট) সব কিছুতেই তার অবৈধ অনুপ্রবেশ সম্ভব হয়।

- **Maintaining Access:** এই ধাপে সমস্ত নিয়ন্ত্রণ চলে আসে হ্যাকারের হাতে। যে ত্রুটি ধরে হ্যাকার ওই সিস্টেমে নিয়ন্ত্রণ নিয়েছে, অন্য হ্যাকার যাতে আবার সেই একইভাবে সেখানে ঢুকে পড়তে না পারে সেজন্য প্রথমেই হ্যাকার উক্ত সিস্টেমের পূর্বের ত্রুটিগুলো সংশোধন করে নেয় এবং পরবর্তীতে নিজের কার্য সাধনের উদ্দেশ্যে সিস্টেমে প্রবেশের জন্য একটি ব্যাকডোর রেখে দেয়। এই অবস্থায় হ্যাকার তার ইচ্ছেমতো তথ্য আপলোড, ডাউনলোড, পরিবর্তন করে সম্পূর্ণ সিস্টেম নিজের দখলে রেখে দিতে পারে।

- **Clearing Tracks:** সর্বশেষ পর্যায়ে এসে হ্যাকার তার ফেলে আসা বিভিন্ন এভিডেন্স মুছে ফেলে, যাতে তার বা তার অবস্থান সম্পর্কে কারও কাছে কোনো তথ্য অবশিষ্ট না থাকে। সে সার্ভার, সিস্টেম, অ্যাপ্লিকেশন লগের সমস্ত হিস্টোরি মুছে ফেলে নিজেকে গোপন করে রাখে আর নিজেকে আড়ালে রেখেই সেই প্রতিষ্ঠানের পুরো সিস্টেম দূর থেকেই নিয়ন্ত্রণ করে।

আর এভাবেই সম্পন্ন হয় একটি সফল সাইবার অ্যাটাক।

অধ্যায়-২

হ্যাকিংয়ের আদ্যপ্রান্ত

২.১ বিশ্বের কিছু হ্যাকার এবং তাদের জীবনী

২.১.১ কেভিন মিটনিক (Kevin Mitnic)

কেভিন মিটনিক হ্যাকিং রাজ্যের সব থেকে প্রভাবশালী হ্যাকার, হ্যাকিংবিষয়ক বইয়ের সর্বোচ্চ বিক্রিত লেখক এবং শীর্ষ সাইবার নিরাপত্তাবিষয়ক বক্তা। কেভিন মিটনিক ৬ই আগস্ট ১৯৬৩ সালে ক্যালিফোর্নিয়া অঙ্গরাজ্যের লস অ্যাঞ্জেলস শহরে জন্মগ্রহণ করেন। তার জাতীয়তা আমেরিকান। পুলিশের হাতে ধরা পড়ার সময় কম্পিউটারবিষয়ক অপরাধে তিনি মোস্ট ওয়ান্টেড ছিলেন।

হ্যাকিংয়ে পদার্পণ : হ্যাকিং বলতে আমরা অধিকাংশ মানুষ কম্পিউটার ব্যবহার করে কোনো যৌগিক বস্তুতে অভিগমন করা বুঝি। হ্যাকিংয়ে কেভিনের হাতেখড়ি হয় মাত্র ১২ বছর বয়সে। তিনি প্রথম কম্পিউটার সিস্টেম ব্যবহার না করে, মোবাইল সিস্টেম ব্যবহার করেন এবং তার প্রথম আক্রমণপন্থা ছিল সোশ্যাল ইঞ্জিনিয়ারিং ও Reverse Engineering। এর মাধ্যমে তিনি বাসে ভ্রমণের পাঞ্চকার্ডপদ্ধতিকে হ্যাক করে বিনা ভাড়ায় ভ্রমণ করতেন।

উল্লেখযোগ্য আক্রমণ : কেভিন এবং তার দুই বন্ধু 'পেসেফিক বেল' নামের প্রতিষ্ঠানের সিস্টেমে প্রবেশ করে। ঐ কোম্পানির ডেটাবেজে ছিল আমেরিকার অধিকাংশ মোবাইল কোম্পানির ফোনকলের নথিপত্র। তারা সেই সময়ে ১ লাখ ৭০ হাজার ইউরো চুরি করে বলে জানায় কোম্পানিটি। নব্বইয়ের দশকে নকিয়া, মোটোরোলা নামের জনপ্রিয় এই দুটি কোম্পানি হ্যাক করতে উদ্যত হলে NEC কোম্পানির সিস্টেম অ্যাডমিন বিষয়টি টের পায় এবং তা FBI-কে অবগত করে।