ইনট্রোশন ডিটেকশন সিস্টেম : নেটওয়ার্কের অতন্দ্র প্রহরী

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

বর্তমান যুগ হলো ডিজিটাল ডিভাইসের যুগ। প্রতিনিয়ত লাখ লাখ ডিজিটাল ডিভাইস নিজেদের মধ্যে যোগাযোগ করে যাচ্ছে। সামাজিক যোগাযোগ থেকে শুরু করে ই-কমার্স– সবকিছুই এখন হয় ইন্টারনেটের মাধ্যমে। এটা যেমন আমাদের জীবনকে করেছে অনেক বেশি স্বাচ্ছন্দ্যপূর্ণ, তেমনি তৈরি করেছে অসংখ্য ঝুঁকি। বিভিন্ন সিস্টেম হ্যাকিং, পাসওয়ার্ড, এমনকি ক্রেডিট কার্ড নম্বর চুরিও এখন খুব নিয়মিত ঘটনা। এ ধরনের ঘটনা প্রতিহত করতে কর্পোরেট প্রতিষ্ঠানগুলো নিয়মিত কাজ করে যাচ্ছে। নেটওয়ার্ক বা সিস্টেম অ্যাডমিনিস্ট্রেটরেরা নতুন নতুন প্রদ্ধতি প্রয়োগ করছেন। কিন্তু শুধু ম্যানুয়ালি নজরদারি করে বড় ধরনের নেটওয়ার্ককে নিরাপদ রাখা সম্ভব নয়। তাদের দরকার এমন একটি পদ্ধতি, যা নিজে থেকেই নেটওয়ার্ক বা সিস্টেমের সব ধরনের কাজ মনিটর করবে এবং কোনো ধরনের সন্দেহজনক অ্যাকটিভিটি সরাসরি নেটওয়ার্ক বা সিস্টেম অ্যাডমিনিস্ট্রেটরকে রিপোর্ট করবে। এ ধরনেরই একটি পদ্ধতি হলো ইনট্রোশন ডিটেকশন সিস্টেম।

ইনট্রোশন ডিটেকশন সিস্টেম (আইডিএস) হলো মূলত এমন একটি ডিভাইস বা সফটওয়্যার, যা সিস্টেম বা নেটওয়ার্কের মধ্যে কোনো ধরনের ম্যালিশাস অ্যাকটিভিটি বা পলিসি ভায়োলেশন চিহ্নিত করে ও নেটওয়ার্ক বা সিস্টেম অ্যাডমিনিস্ট্রেটরকে রিপোর্ট করে। এটির মূল কাজ ম্যালিশাস ডিটেক্ট করা, লগ তৈরি ও রিপোর্ট করা। এ ছাড়া নেটওয়ার্ক বা সিস্টেম অ্যাডমিনিস্ট্রেটরেরা এটাকে কোনো সিস্টেমের ত্রুটি খুঁজে বের করা বা সিকিউরিটি থ্রেট ডকুমেন্ট করার কাজেও ব্যবহার করে থাকে।

যেভাবে কাজ করে : সব ধরনের আইডিএসই সাধারণত দুইভাবের যেকোনো একভাবে কাজ করে থাকে।

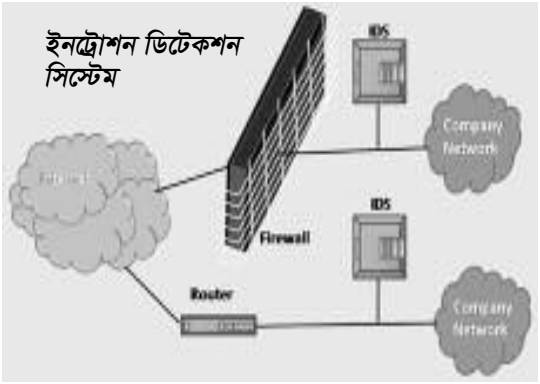
স্ট্যাটিক্যাল অ্যানুম্যালাইভিত্তিক আইডিএস : এ ধরনের আইডিএসে নেটওয়ার্কের সাধারণ আচরণ রেকর্ড করা হয়। যেমন এ নেটওয়ার্কে সাধারণত কেমন ব্যান্ডউইডথ ব্যবহার হয়, কী ধরনের প্রটোকল ব্যবহার করা হয়, কী কী পোর্ট ব্যবহার করা হয় ও কী কী ডিভাইস ব্যবহার হয়। এখন যদি দেখা যায় এই সাধারণ আচরণ থেকে নতুন কোনো প্যাটার্ন দেখা যায়, তবে আইডিএস তা সাসপিসিয়াস হিসেবে ডিটেক্ট করে ও নেটওয়ার্ক অ্যাডমিনিস্ট্রেটরকে রিপোর্ট করে। এ ধরনের আইডিএস মূলত নেটওয়ার্কের ব্যবহার স্ট্যাটিক্যালি রেকর্ড করে ও এ ধরনের স্ট্যাটিক্যালি রেকর্ডের ওপর ভিত্তি করে অ্যানোম্যালাই বা বিপজ্জনক আচরণ খুঁজে বের করে।

সিগনেচারভিত্তিক আইডিএস : আরেক ধরনের আইডিএস আছে, যা আগে থেকেই কনফিগার করা থাকে। যদি নেটওয়ার্ক বা সিস্টেমের আচরণ কনফিগার করা প্যাটার্নের সাথে মিলে যায়, তবে তা ডিটেক্ট করে অ্যাডমিনিস্ট্রেটরের কাছে রিপোর্ট করে।

প্রকারভেদ

হোস্টভিত্তিক আইডিএস : এ ধরনের আইডিএস পদ্ধতিতে সফটওয়্যারটি যেকোনো হোস্ট কমপিউটারে ইনস্টল করা থাকে এবং নিজে থেকেই কাজ করতে পারে। হোস্ট সিস্টেম, নিজের লগ ফাইল ও অন্যান্য সিস্টেম ইভেন্ট ইনভেসটিগেট করে সাধারণত অ্যালার্ট জেনারেট করে থাকে। হোস্টভিত্তিক আইডিএস শুধু একটি কমপিউটারে ট্রাফিক অ্যানালাইসিস করে। এ ছাড়া সিস্টেমের ফাইল ইন্টিগ্রিটি পরীক্ষা করে ও সন্দেহজনক প্রসেসকে পর্যবেক্ষক করে।

নেটওয়ার্কভিত্তিক আইডিএস : একটি নেটওয়ার্কভিত্তিক আইডি সিস্টেম পুরো একটি নেটওয়ার্ক সেগমেন্টের জন্য কাজ করে। সাধারণত নেটওয়ার্ক থেকে যেসব প্যাকেট ইন বা আউট হয় তা প্রমিসকোয়াস মোডে ক্যাপচার করে। নেটওয়ার্কভিত্তিক আইডিএসে পুরো নেটওয়ার্কের অ্যাকটিভিটি সম্পর্কে ধারণা পাওয়া যায়। তবে হোস্টভিত্তিক সিস্টেম ও নেটওয়ার্কভিত্তিক সিস্টেমের নিজ নিজ ভালো ও দুর্বল দিক রয়েছে। তাই প্রয়োজন অনুযায়ী দুটোর সমন্বয়ের মাধ্যমে সবচেয়ে ভালো ফল পাওয়া সম্ভব।



ইনট্রোশন ডিটেকশন সিস্টেম

গ্রাফিক্যাল টুল

একটি ছবি সাধারণত হাজার শব্দের মূল্য হিসেবে বিবেচিত হয়। গ্রাফিক্যাল টুল ব্যবহার করে সন্দেহভাজন তথ্য রেন্ডার করে নেটওয়ার্ক ট্রাফিক ড্র করা খুব সহজেই উপস্থাপন করা যায়। ফলে খুব সহজেই নিরাপত্তা বিশ্লেষক নেটওয়ার্কে কোনো অ্যানোম্যালাই ডিটেক্ট করতে পারে।

EtherApe : বর্তমানে লাইভ ট্রাফিক বা প্যাকেট ক্যাপচার, ফাইল সার্চ ও সিস্টেমের মধ্যে সম্পর্ক স্থাপন করতে পারে এবং সে অনুযায়ী তথ্য গ্রাফিক্যালি উপস্থাপন করতে পারে। এটি ওপেন সোর্স ইউনিক্স প্রকল্প। এটা বিভিন্ন ধরনের রং ব্যবহার করে তথ্য মনোযোগ আকর্ষণ করে, নাম রেজ্যুলেশন সমর্থন করে ও প্যাকেট ইনভেস্টিগেশনের সময় ডিপ প্যাকেট ফিল্টার কনফিগার করা সাপোর্ট করে।

NetGrok : জাভা সমর্থনকারী যেকোনো অপারেটিং সিস্টেমের ওপর রান করতে পারে। রিয়েল টাইম পর্যবেক্ষণ ও প্যাকেট ক্যাপচার ফাইল পড়া সমর্থন করে। অভ্যন্তরীণ নেটওয়ার্কের দৃষ্টিকোণ থেকে নেটওয়ার্ক অ্যাকটিভিটি পর্যবেক্ষণ করা হয় এবং নেটওয়ার্কের গতির ওপর ভিত্তি করে বিভিন্ন রঙিন কোডিং করা হয়।

ফলস পজিটিভ ও ফলস নেগেটিভ : যারা আইডিএস নিয়ে কাজ করে থাকেন তাদের কাছে ফলস পজিটিভ একটি পরিচিত শব্দ। ফলস পজিটিভ হলো যখন আইডিএস কোনো একটি নিরাপদ ইভেন্টকে অনিরাপদ বা ম্যালিশাস ইভেন্ট হিসেবে শনাক্ত করে ও অ্যাডমিনিস্ট্রেটরকে সেই হিসেবে ইভেন্টটির রিপোর্ট করে। ফলস নেগেটিভ হলো কোনো একটি আইডিএস কোনো একটি ম্যালিশাস অ্যাকটিভিটিকে যদি শনাক্ত না করতে পারে, তবে তাকে ফলস নেগেটিভ বলে থাকি। সাধারণত একটি আইডিএস কতটা ভালো তা বুঝাতে তার ফলস পজিটিভ ও নেগেটিভ রেট কতটা কম তার মাধ্যমে বুঝানো হয়।

আইডিএসের সীমাবদ্ধতা

* নয়েজ ও অতিরিক্ত ত্রুটিপূর্ণ প্যাকেট যদি নেটওয়ার্কে বেশি থাকে, তবে আইডিএস সঠিকভাবে কাজ করতে পারে না।
* সিগনেচারভিত্তিক আইডিএসকে নিয়মিত আপডেট না করলে নতুন নতুন ভলনিয়াবিলিটি শনাক্ত করতে পারবে না।
* অনেক সময় আনেক ধরনের অ্যাটাক শুধু কোনো স্পেসিফিক সফটওয়্যারকেন্দ্রিক হয়। এ ধরনের অ্যাটাক প্রতিহত করতে আইডিএসের প্রতিরক্ষা ব্যবস্থা কিছুটা দুর্বল।

কীভাবে আইডিএসকে বাইপাস করা সম্ভব : কভার্ট চ্যানেলের মাধ্যমে সাধারণত আইডিএস ও ফায়ারওয়াল ব্যবস্থা ভেদ করা সম্ভব। এ গোপন চ্যানেল নেটওয়ার্কের কোনো ফায়ারওয়াল ও আইডিএসের সতর্ক বিনা মেশিনের মধ্যে তথ্য ডাটা আদান-প্রদানের জন্য একটি খুব সহজ কার্যকর প্রক্রিয়া। এর নেটওয়ার্কের ট্রাফিককে আপাতভাবে অনেক সাধারণ বলে মনে হয়। ফলে আইডিএস এটাকে ম্যালিশাস হিসেবে শনাক্ত করে না। এ পদ্ধতিতে বিভিন্ন টিসিপি ও আইপি হেডার বিভিন্ন নিয়ন্ত্রণ ক্ষেত্রে প্রকৃত তথ্য গোপন করে এবং পেলোডে সাধারণ তথ্য বহন করে একটি নির্দোষ প্যাকেট হিসেবে নেটওয়ার্কে ঢুকে। কিন্তু টিসিপি ও আইপি হেডার ইনফরমেশন দিয়ে নিজেদের রিকনস্ট্রাক্ট করে ও নেটওয়ার্কের ক্ষতিসাধন করে।

শেষ কথা

কোনো সন্দেহ নেই যে প্রযুক্তির এ দুনিয়ায় প্রতিনিয়ত অনাকাঙ্ক্ষিত অনুপ্রবেশের ঘটনা বাড়ছে। ই-কমার্সের এ যুগে নিজেকে লুকানোরও কোনো ব্যবস্থা নেই। তাই নিজেকে এবং নিজের প্রযুক্তির প্রতিরক্ষাকে আরও শক্তিশালী করা ছাড়া আর কোনো পথ নেই। তাই ইনট্রোশন ডিটেকশন সিস্টেম হতে পারে আপনার ফার্স্ট লাইন অব ডিফেন্স কজ

ফিডব্যাক : jabedmorshed@yahoo.com