পারফরম্যান্স মনিটর ও নেটওয়ার্ক ডিফেন্স

কে এম আলী রেজা

নেটওয়ার্কের নিরাপত্তা বিধান নিঃসন্দেহে একটি গুরুত্বপূর্ণ কাজ। উইন্ডোজ অপারেটিং সিস্টেমে বিল্ট-ইন টুল যেমন পারফরম্যান্স মনিটরের (Perfmon) সহযোগিতা নিয়ে কমপিউটার তথা নেটওয়ার্ককে বাইরের আক্রমণ থেকে বেশি সুরক্ষিত করা যায়। এসব টুল যথাযথভাবে কনফিগার করা থাকলে কমপিউটার নিজেই অনেক ঝুঁকিকর নেটওয়ার্ক আক্রমণ থেকে নিজেকে নিরাপদ করতে পারে। এ লেখায় ইথারনেট নেটওয়ার্কে আক্রমণের ফলে এআরপি (অ্যাড্রেস রেজ্যুলেশন প্রোটোকল) পয়জনিং (poisoning) বিষয়টি তুলে ধরা হয়েছে এবং বর্ণনা করা হয়েছে কীভাবে পারফরম্যান্স মনিটরের সাহায্যে এআরপি পয়জনিং রোধ করা যায়।

বাইরে থেকে বিভিন্ন ধরনের আক্রমণের কারণে নেটওয়ার্ক সবসময় ঝুঁকির মধ্যে থাকে। এ কারণে নেটওয়ার্ককে সুরক্ষা দানের জন্য নিয়মিতভাবে এর বিভিন্ন কার্যক্রম পর্যবেক্ষণ করতে হয়। যথাযথভাবে কনফিগার করা থাকলে পারফরম্যান্স মনিটর নেটওয়ার্কের বিভিন্ন কর্মকাণ্ডের ওপর নিয়মিতভাবে রিপোর্ট তৈরি করে যা ট্রাবলশুটিংয়ে কাজে লাগে। স্ক্রিপ্টের মাধ্যমেও এ টুলটি নেটওয়ার্ক মনিটরের কাজ করতে পারে এবং বাইরে থেকে পরিচালিত আক্রমণ থেকে নেটওয়ার্ককে নিরাপদ রাখতে পারে।

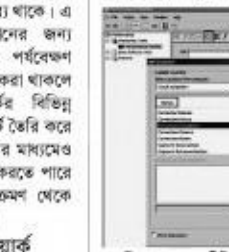
ডিনায়্যাল অব সার্ভিস নেটওয়ার্ক অ্যাটাক

উদাহরণ হিসেবে এখানে নেটওয়ার্কের বহু পরিচিত ডিনায়্যাল অব সার্ভিস (DoS) অ্যাটাককে বিবেচনায় আনা হয়েছে। এ ধরনের অ্যাটাক নেটওয়ার্কে ভুয়া টিসিপি সিন্ক প্যাকেট (TCP SYN)-এর ব্যাপক উপস্থিতি লক্ষ করা যায়, যা ভুয়া ডাটা প্যাকেটের বন্যা হিসেবে পরিচিত। এ ধরনের নেটওয়ার্ক আক্রমণ অনেক পুরনো এবং বহুল পরিচিত হওয়া সত্ত্বেও এর প্রতিকারে উইন্ডোজ অপারেটিং সিস্টেমে এখন তেমন কোনো কার্যকর বিল্ট-ইন ব্যবস্থা নেই।

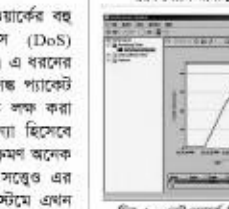
ডিনায়্যাল অব সার্ভিসের মতো হামলা থেকে নেটওয়ার্ককে নিরাপদ রাখার জন্য নেটওয়ার্ক ফায়ারওয়াল এবং রাউটারকে কনফিগার করা যায়। তবে এখানে দেখানো হয়েছে কীভাবে নেটওয়ার্কের হোস্ট কমপিউটার পর্যায়ে এসব আক্রমণ প্রতিরোধ করা যায়। নেটওয়ার্কে কোনো আক্রমণ বাস্তব সময়ে (real-time) নিরূপণ এবং আক্রমণ সম্পর্কিত মূল্যবান তথ্য ক্যাপচার করা আমাদের পক্ষে সম্ভব নয়। এ কাজটি করার জন্য কমপিউটারের 'পারফরম্যান্স মনিটর' নামে টুলের সাহায্য নেয়া হয়েছে।

পারফরম্যান্স মনিটর প্রথমে একটি ডাটা কালেক্টর সেট তৈরি করবে। ডাটা কালেকশনের জন্য পূর্বনির্ধারিত কোনো মনিটরিং প্যারামিটারের মান (threshold) অতিক্রম করলেই সংশি-ষ্ট স্ক্রিপ্ট বা প্রোগ্রামটি চালু হয়ে যাবে। প্রক্রিয়াটি আপাত দৃষ্টিতে জটিল মনে হলেও বাস্তবে এর কনফিগারেশন বেশ সহজ।

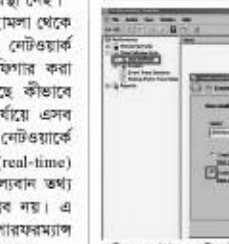
পারফরম্যান্স মনিটর স্ক্রিপ্ট সফলভাবে কোনো নেটওয়ার্ক আক্রমণ শনাক্ত করতে পারে কি না তা পরীক্ষার জন্য পরীক্ষামূলকভাবে আর্টিফিসিয়াল ডিনায়্যাল অব সার্ভিস (DoS) আক্রমণ তৈরি করতে হবে। এ ধরনের আক্রমণ তৈরির জন্য টুল হিসেবে Ettercap-এর সাহায্য নেয়া যেতে পারে। তবে Ettercap হ্যাকিং টুলটির ব্যবহার করতে হবে কোনো পরীক্ষামূলক নেটওয়ার্কে। কোনো অবস্থাতেই বাণিজ্যিক বা



চিত্র-১ : সম্ভাব্য টিসিপি সিন্ক আক্রমণ নির্ণয়ের জন্য পারফরম্যান্স মনিটরে কাউন্টার সেট করা হয়েছে



চিত্র-২ : নেটওয়ার্কে টিসিপি সিন্ক অ্যাটাকের উপস্থিতি



চিত্র-৩ : ইউজার ডিফাইন্ডডাটা কালেক্টর সেট তৈরিকরণ

ফাংশনাল গুরুত্বপূর্ণ নেটওয়ার্কে এ ধরনের টুল ব্যবহার করা যাবে না। তাহলে ওইসব নেটওয়ার্ক মূল্যবান ডাটা ও সেটিং ঝুঁকির মধ্যে পড়তে পারে।

অ্যাটাক সিগনেচার

নেটওয়ার্ক অ্যাটাক প্রতিরোধের আগে আপনাকে সম্ভাব্য হামলা সম্পর্কে সজাগ থাকতে হবে এবং এগুলো যথাসময়ে শনাক্ত করতে হবে। গোয়েন্দাদের ভাষায় একে বলা হয় অ্যাটাক সিগনেচার। নেটওয়ার্ক পারফরম্যান্স মনিটরের ওয়াচ লিস্টে কাউন্টার যোগ করে নেটওয়ার্ক হামলা সহজেই শনাক্ত করা যায়। নেটওয়ার্ক হামলা হলে এসব কাউন্টার বা ইন্ডিকেটরের মান পরিবর্তন হয় এবং তা সহজেই নেটওয়ার্ক অ্যাডমিনিস্ট্রেটরের নজরে আসে। কাউন্টারের অস্বাভাবিক অবস্থা দেখে ব্যবহারকারী নেটওয়ার্ক অ্যাটাক শনাক্ত করতে পারেন এবং তা প্রতিরোধে প্রয়োজনীয় ব্যবস্থা নিতে পারেন। চিত্র-১-এ ভুয়া টিসিপি সংযোগ নির্ণয়ের জন্য পারফরম্যান্স মনিটরে TCPv4-এর একটি কাউন্টার সেট করা হয়েছে।

টিসিপি সিন্ক (TCP SYN) ফ্লাড অ্যাটাকের ক্ষেত্রে অ্যাটাক সিগনেচার হিসেবে অসংখ্য টিসিপি সংযোগের উপস্থিতি পারফরম্যান্স মনিটরে দেখা যাবে। পারফরম্যান্স মনিটরে টিসিপি সংযোগের ব্যাপক সংখ্যা নিশ্চয় স্বাভাবিক কোনো বিষয় নয়। একটি স্বাভাবিক নেটওয়ার্কে টিসিপি সংযোগের সাথে একে তুলনা করতে বুঝতে অসুবিধা হবে না যে এটি নেটওয়ার্ক অ্যাটাকের কারণে সংঘটিত হয়েছে। চিত্র-২-এ পারফরম্যান্স মনিটরে দেখা যাচ্ছে টিসিপি নেটওয়ার্ক সংযোগের সংখ্যা সর্বোচ্চ ৪০ হাজার পর্যন্ত উন্নীত। এ ধরনের অস্বাভাবিক সংখ্যক সংযোগ থেকে বুঝা যায় বাইরে থেকে নেটওয়ার্ক অ্যাটাকের কারণে এ অস্বাভাবিক অবস্থা তৈরি হয়েছে।

নেটওয়ার্ক মনিটরিং

নেটওয়ার্ক অ্যাটাকের ধরন এবং এর উপস্থিতি জানার পর তা প্রতিরোধের জন্য পারফরম্যান্স মনিটর টুলের ইউজার ডিফাইন্ড ডাটা কালেক্টর সেট (UDDCS)-এর সাহায্য নেয়া যেতে পারে। ইউডিডিসিএসের সাহায্যে আমরা যেকোনো সিস্টেম কাউন্টার নিয়মিতভাবে মনিটর করতে পারি। নেটওয়ার্কে কোনো হামলা হলে কাউন্টারের মানের পরিবর্তন হবে এবং এর ওপর ভিত্তি করে আমরা সতর্কীকরণ (alert) বার্তা তৈরি করতে পারি অথবা আমাদের পছন্দমতো এ সংক্রান্ত কোনো স্ক্রিপ্ট সিস্টেমে রান করাতে পারি। ইউডিডিসিএস তৈরির জন্য পারফরম্যান্স মনিটরের উইন্ডোতে গিয়ে Data Collector Sets-এর অধীনে User Defined-এর ওপর মাউসের ডান ক্লিক করুন। পপআপ মেনু থেকে প্রাপ্ত উইন্ডোতে নতুন ডাটা কালেক্টর সেট হিসেবে SYN flood attack detector তৈরি করুন (চিত্র-৩)।

নিজেদের তৈরি কাউন্টার সেট ব্যবহারের জন্য ▸

চিত্র-৩-এ দ্বিতীয় অর্থাৎ ম্যানুয়াল অপশনটি সিলেক্ট করতে হবে। এবার Next বাটনে ক্লিক করে পরবর্তী স্ক্রিনের পারফরম্যান্স কাউন্টার অ্যালার্ট অপশনটি সিলেক্ট করতে হবে (চিত্র-৪)।

এবার Next বাটনে আবার ক্লিক করে কাঙ্ক্ষিত কাউন্টার এবং তার জন্য একটি সীমাসূচক সর্বোচ্চ মান (threshold) নির্ধারণ করতে হবে। এক্ষেত্রে কাউন্টারের সর্বোচ্চ মান ২৫ হাজার সেট করা হয়েছে।

আবার Next বাটনে ক্লিক করে ডাটা কালেক্টর সেট প্রোপার্টিজ অপশনটি সিলেক্ট করুন। এবার Finish বাটনে ক্লিক করুন এবং ডাটা সেট মনিটরিংয়ের জন্য একটি সিস্টাল নির্ধারণ করে দিন। আমরা যদি চাই সিস্টেমে মনিটরিং টাস্কটি ব্যাকগ্রাউন্ডে সবসময় সক্রিয় থাকবে তাহলে শুধু একে চালু করলেই হবে, প্রসেসটি বন্ধ করার জন্য কোনো শর্তারোপ করার প্রয়োজন নেই। বিকল্প পদ্ধতি হিসেবে ডাটা কালেক্টর সেটটি এমনভাবে কনফিগার করতে পারে, যাতে এটি দিনের একটি নির্দিষ্ট সময় চালু থাকবে, বাকি সময় এটি বন্ধ থাকবে। তবে নেটওয়ার্কের অন-গোয়িং কর্মকাণ্ড মনিটরিং করার স্বার্থে প্রসেসটিকে সার্বক্ষণিকভাবে চালু রাখাই শ্রেয়।

টাস্ক সিডিউল সেট করার পর Ok বাটনে ক্লিক করুন। এ পর্যায়ে আপনার সামনে পারফরম্যান্স মনিটরের প্রধান উইন্ডো ফিরিয়ে আনা হবে। এখানে আপনাকে ডাটা কালেক্টর সেটসের অধীনে DataCollector01-এ মাউসের ডান ক্লিক করতে হবে।

এবার আপনাকে স্যাম্পলিং ইন্টারভেল কনফিগার করতে হবে। এ উদাহরণে এক মিনিট অন্তর একবার ডাটা ক্যাপচার করার জন্য once-per-minute স্যাম্পলিং ইন্টারভেল বেছে নেওয়া হয়েছে।

এবার প্রোপার্টিজ উইন্ডোর Alert Action ট্যাবটি সিলেক্ট করে অ্যালার্ট এমনভাবে কনফিগার করতে হবে যাতে এটি নেটওয়ার্ক হামলা সম্পর্কিত সতর্কবার্তা ইভেন্ট লগে এন্ট্রি দিতে পারে।

এবার মনিটরের প্রধান উইন্ডোর Perfmon→Data Collector Sets→User Defined→SYN Flood Attack Detector→right-click→Start থেকে টাস্ক বা প্রসেসটি চালু করুন। এ পর্যায়ে Ettercap বা অনুরূপ কোনো প্রোগ্রাম রান করে একটি আর্টিফিসিয়াল নেটওয়ার্কে অ্যাটাক চালু করতে পারেন। নেটওয়ার্ক অ্যাটাকের কারণে আপনার সেট করা কাউন্টারে কোনো পরিবর্তন এসেছে কি না তা দেখার জন্য Event Viewer→Applications and Services Log→Microsoft→Windows→Diagnosis-PLA থেকে ID 2031 ইভেন্টটি অনুসন্ধান করুন।

চিত্র-৪ : পারফরম্যান্স কাউন্টার অ্যালার্ট অপশন সিলেক্ট করা

চিত্র-৫ : স্যাম্পলিং ইন্টারভেল সেট করার উইন্ডো

চিত্র-৬ : মনিটরিং টাস্কের সাথে অ্যালার্ট ফিল্টার যুক্তকরণ

এখানে উলে-খ করা প্রয়োজন, ইভেন্ট ID 2031 হচ্ছে একটি জেনেরিক অ্যালার্ট, যা সিস্টেম অ্যাডমিনিস্ট্রেটর যেকোনো শর্ত বা অবস্থার ক্ষেত্রে একে কনফিগার বা ডিফাইন করতে পারে।

মনিটরিং টাস্কের সাথে অ্যালার্ট যুক্তকরণ

এবার মনিটরিং টাস্ককে নেটওয়ার্ক অ্যাটাক অ্যালার্টের সাথে যুক্ত করার পালা। যখনই উইন্ডোজ ইভেন্ট লগে (Event Log) একটি অ্যালার্ট যোগ করা হয়, তখনই এটি একটি টাস্ক ট্রিগার চালু করে। উদাহরণস্বরূপ এখানে ID 2031-এর ওপর মাউসের ডান ক্লিক করে পপআপ মেনু থেকে Attach Task to This Event সিলেক্ট করুন। পরপর দু'বার Next বাটনে ক্লিক করে Action প্যানে যেতে হবে। এখানে Start a Program-এ ক্লিক করে এরপর Next বাটনে ক্লিক করুন। এ উদাহরণে অ্যালার্ট স্ক্রিপ্ট হিসেবে c:\admin\scripts\synflood-forensics.bat প্রোগ্রামটি রান করা হয়েছে।

টাস্কের সাথে অ্যালার্ট যুক্ত হওয়ার পর অ্যালার্ট মেসেজ C:\Windows\System32\Tasks\Event Viewer Tasks-এ সংরক্ষিত হতে থাকবে। এ পর্যায়ে একটি ফাংশনাল TCP SYN flood মনিটর কমপিউটারে পেয়ে যাবেন। নেটওয়ার্কে টিসিপি সংযোগের সংখ্যা বা সেশন ২৫ হাজারের সীমা অতিক্রম করা মাত্রই মনিটরটি ধরে নেবে নেটওয়ার্কে অ্যাটাক হয়েছে। এটি তাৎক্ষণিকভাবে ডাটা ক্যাপচার প্রক্রিয়া শুরু করবে যা আপনি ইভেন্ট ভিউতে গিয়ে দেখতে পারবেন।

ফিডব্যাক : kazisham@yahoo.com