অধ্যায়-২ সিস্টেম এবং নেটওয়ার্ক সিকিউরিটি

SOS অতি সংক্ষিপ্ত প্রশ্নোত্তর ঃ

*** ১। সিস্টেম নিরাপত্তা বলতে কী বুঝায়?**

উত্তর ঃ সিস্টেম নিরাপত্তা (System Security) বলতে একটি কম্পিউটার সিস্টেমের হার্ডওয়্যার, সফটওয়্যার এবং এর মধ্যে থাকা ডাটাকে অননুমোদিত প্রবেশ, ক্ষতি বা চুরি থেকে রক্ষা করার সামগ্রিক প্রক্রিয়াকে বোঝায়।

***** ২। কাজ লেখ; IPS, VPN?** বাকাশিবো- ২০২৫

উত্তর ঃ **IPS ঃ** IPS (Intrusion Prevention System) বা অনুপ্রবেশ প্রতিরোধ ব্যবস্থা হলো একটি অত্যন্ত গুরুত্বপূর্ণ ডিভাইস বা সফটওয়্যার। এটি নেটওয়ার্ক ট্রাফিক প্রতিনিয়ত মনিটর করে এবং কোনো ক্ষতিকারক বা সন্দেহজনক কার্যকলাপ শনাক্ত করার সাথে সাথে তা স্বয়ংক্রিয়ভাবে বন্ধ করে দেয়।

VPN ঃ VPN (Virtual Private Network) বা ভার্চুয়াল প্রাইভেট নেটওয়ার্ক একটি শক্তিশালী ঢাল হিসেবে কাজ করে। এটি পাবলিক ইন্টারনেট ব্যবহারের সময় আপনার ডাটাকে একটি সুরক্ষিত এবং এনক্রিপ্টেড (Encrypted) টানেলের মধ্য দিয়ে পাঠায়।

**** ৩। ফায়ারওয়াল (Firewall) কী?**

উত্তর ঃ ফায়ারওয়াল হলো সাইবার নিরাপত্তার একটি অতি গুরুত্বপূর্ণ অংশ, যা একটি সুরক্ষিত অভ্যন্তরীণ নেটওয়ার্ক এবং একটি অনিরাপদ বাহ্যিক নেটওয়ার্কের (যেমন- ইন্টারনেট) মধ্যে দেয়াল বা প্রহরী হিসেবে কাজ করে।

**** ৪। ফায়ারওয়াল প্রধানত কয় প্রকার ও কী কী?** বাকাশিবো- ২০২৪পরি

উত্তর ঃ কাজের পদ্ধতি বা ফিল্টারিং প্রযুক্তির ওপর ভিত্তি করে ফায়ারওয়াল প্রধানত ৫ প্রকার যথা;

i) প্যাকেট ফিল্টারিং ফায়ারওয়াল (Packet Filtering Firewall)

ii) সার্কিট-লেভেল গেটওয়ে (Circuit-Level Gateway)

iii) স্টেটফুল ইন্সপেকশন ফায়ারওয়াল (Stateful Inspection Firewall)

iv) প্রক্সি ফায়ারওয়াল বা অ্যাপ্লিকেশন ফায়ারওয়াল (Proxy Firewall)

v) নেক্সট-জেনারেশন ফায়ারওয়াল (Next-Generation Firewall - NGFW)

**** ৫। Treat (হুমকি) কী?**

উত্তর ঃ Threat বা হুমকি বলতে এমন কোনো সম্ভাব্য বিপদ বা ঘটনাকে বোঝায়, যা কোনো কম্পিউটার সিস্টেম, নেটওয়ার্ক বা তথ্যের ক্ষতি করতে পারে। সহজ কথায়, ডিজিটাল জগতের যেকোনো ক্ষতিকারক কর্মকাণ্ড বা

পরিস্থিতি, যা তথ্যের গোপনীয়তা, অখণ্ডতা বা প্রাপ্যতা নষ্ট করার ক্ষমতা রাখে, তাকেই হুমকি বলা হয়।

***** ৬। DDoS কী?** বাকাশিবো- ২০২৪'পরি, ২৫

উত্তর ঃ DDoS এর পূর্ণরূপ হলো Distributed Denial of Service.

এটি এমন এক ধরণের সাইবার আক্রমণ, যেখানে একটি নির্দিষ্ট ওয়েবসাইট, সার্ভার বা নেটওয়ার্ককে লক্ষ্য করে অসংখ্য ভুয়া ট্রাফিক বা রিকোয়েস্ট পাঠানো হয়। এর ফলে ওই সার্ভারটি অতিরিক্ত লোড সহ্য করতে না পেরে স্লো হয়ে যায় বা পুরোপুরি বন্ধ (Crash) হয়ে যায়।

SOS সংক্ষিপ্ত প্রশ্নোত্তর ঃ

*** ১। সিস্টেম ও নেটওয়ার্ক নিরাপত্তার প্রধান দিকগুলো কী কী?**

বাকাশিবো- ২০২৫

উত্তর ঃ সিস্টেম নিরাপত্তার প্রধান দিকগুলো নিম্নরূপঃ

i) অ্যাক্সেস কন্ট্রোল (Access Control)

ii) ইউজার প্রোফাইল ও প্রিভিলেজ ম্যানেজমেন্ট

iii) ফাইল সিস্টেম ও ডাটা সুরক্ষা

iv) ম্যালওয়্যার ও থ্রেট সুরক্ষা (Threat Protection)

v) সিস্টেম অডিটিং ও মনিটরিং (Auditing, Logging)

vi) নিয়মিত আপডেট ও প্যাচ ম্যানেজমেন্ট

vii) ব্যাকআপ ও ডিজাস্টার রিকভারি

নেটওয়ার্ক নিরাপত্তার প্রধান দিকগুলো নিম্নরূপ ঃ

i) ফায়ারওয়াল (Firewall)

ii) নেটওয়ার্ক এক্সেস কন্ট্রোল (Network Access Control - NAC)

iii) ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN)

iv) অনুপ্রবেশ শনাক্তকরণ ও প্রতিরোধ ব্যবস্থা (IDS/IPS)

v) নেটওয়ার্ক সেগমেন্টেশন (Network Segmentation)

vi) ওয়্যারলেস সিকিউরিটি (Wireless Security)

vii) অ্যাপলিকেশন সিকিউরিটি (Application Security)

**** ২। ফায়ারওয়ালের কাজ লেখ।**

উত্তর ঃ ফায়ারওয়ালের কাজগুলো নিম্নরূপ ঃ

১. ইনকামিং ট্রাফিক ফিল্টারিং ঃ ফায়ারওয়ালের সবচেয়ে গুরুত্বপূর্ণ কাজ হলো ইন্টারনেট থেকে আপনার কম্পিউটারে আসা সমস্ত তথ্য বা ডেটা প্যাকেট পরীক্ষা করা। এটি ক্ষতিকারক ওয়েবসাইট বা হ্যাকারদের পাঠানো সন্দেহজনক রিকোয়েস্টগুলো শনাক্ত করে এবং সেগুলোকে আটকে দেয়।

২. অননুমোদিত প্রবেশ রোধ ঃ হ্যাকাররা সবসময় ইন্টারনেটের মাধ্যমে বিভিন্ন কম্পিউটারে ঢোকার জন্য 'খোলা পথ' বা পোর্ট (Port) খোঁজে। ফায়ারওয়াল অপ্রয়োজনীয় সব পোর্ট বন্ধ করে রাখে, ফলে হ্যাকাররা চাইলেও আপনার সিস্টেমে অনধিকার প্রবেশ করতে পারে না।

৩. আউটগোয়িং ট্রাফিক মনিটরিং ঃ ফায়ারওয়াল শুধু বাইর থেকে আসা তথ্যই চেক করে না, বরং আপনার কম্পিউটার থেকে বাইরে কী তথ্য যাচ্ছে তাও নজরে রাখে। যদি কোনো ম্যালওয়্যার আপনার অজান্তে আপনার গোপন তথ্য ইন্টারনেটে পাচার করার চেষ্টা করে, তবে ফায়ারওয়াল তা শনাক্ত করে বাধা দিতে পারে।

৪. ম্যালওয়্যার ও ভাইরাসের বিস্তার রোধ ঃ অনেক ভাইরাস বা ওয়ার্ম নেটওয়ার্কের মাধ্যমে এক কম্পিউটার থেকে অন্য কম্পিউটারে ছড়িয়ে পড়ে।

ফায়ারওয়াল এই ধরণের ক্ষতিকারক সফটওয়্যারের যাতায়াত পথ বন্ধ করে দিয়ে নেটওয়ার্কের অন্যান্য ডিভাইসকে সুরক্ষিত রাখে।

৫. প্রক্সি ও কন্টেন্ট ফিল্টারিং ঃ অনেক উন্নত ফায়ারওয়াল (যেমন- কর্পোরেট ফায়ারওয়াল) নির্দিষ্ট কিছু ওয়েবসাইট বা অ্যাপ্লিকেশন ব্লক করতে পারে। উদাহরণস্বরূপ, কোনো অফিস চাইলে তাদের নেটওয়ার্কে সোশ্যাল মিডিয়া সাইটগুলো ব্লক করে রাখতে পারে, যা ফায়ারওয়ালের মাধ্যমেই করা হয়।

৬. আইপি অ্যাড্রেস ব্লকিং ঃ যদি কোনো নির্দিষ্ট আইপি অ্যাড্রেস থেকে বারবার সাইবার আক্রমণের চেষ্টা করা হয়, তবে ফায়ারওয়াল সেই নির্দিষ্ট আইপি-কে কালো তালিকাভুক্ত (Blacklist) করে চিরতরে ব্লক করে দিতে পারে।

**** ৩। NGFW ব্যাখ্যা কর।** বাকাশিবো- ২০২৫

উত্তর ঃ NGFW-এর পূর্ণরূপ হলো Next-Generation Firewall (নেক্সট-জেনারেশন ফায়ারওয়াল)। এটি হলো প্রথাগত বা ট্র্যাডিশনাল ফায়ারওয়ালের একটি উন্নত এবং আধুনিক সংস্করণ, যা বর্তমান যুগের জটিল সাইবার হামলা মোকাবিলা করার জন্য তৈরি করা হয়েছে। সাধারণ ফায়ারওয়াল যেখানে কেবল আইপি (IP) অ্যাড্রেস এবং পোর্ট নম্বর দেখে ডেটা ফিল্টার করত, সেখানে NGFW ডেটার গভীরে গিয়ে পরীক্ষা করতে পারে। আধুনিক হ্যাকাররা এখন সাধারণ পোর্ট বা আইপি ব্লক এড়িয়ে যেতে পারে। তারা ম্যালওয়্যারকে সাধারণ ডেটা প্যাকেটের ভেতরে লুকিয়ে পাঠায়। এই ধরণের সুক্ষ্ম এবং শক্তিশালী আক্রমণ (যেমন- Ransomware) প্রতিরোধের জন্য NGFW বর্তমানে প্রতিটি বড় প্রতিষ্ঠানের জন্য অপরিহার্য।

SOS রচনামূলক প্রশ্নোত্তর ঃ

**** ১। ফারারওয়ালের প্রকারভেদ বর্ণনা কর।**

উত্তর ঃ কাজের পদ্ধতি বা ফিল্টারিং প্রযুক্তির ওপর ভিত্তি করে ফায়ারওয়াল প্রধানত ৫ প্রকার যথা,

১) প্যাকেট ফিল্টারিং ফায়ারওয়াল (Packet Filtering Firewall) ঃ এটি সবচেয়ে পুরনো এবং সাধারণ ধরণের ফায়ারওয়াল। এটি প্রতিটি ডেটা প্যাকেটের আইপি (IP) অ্যাড্রেস, পোর্ট নম্বর এবং প্রোটোকল চেক

করে। যদি তা আগে থেকে সেট করা নিয়মের সাথে মিলে যায়, তবেই তাকে ঢুকতে দেয়।

সুবিধাঃ এটি খুব দ্রুত কাজ করে।

২) সার্কিট-লেভেল গেটওয়ে (Circuit-Level Gateway) ঃ এটি ডেটা প্যাকেটের ভেতরের তথ্য পরীক্ষা করার বদলে নেটওয়ার্কের সংযোগ বা সেশন (TCP Handshake) বৈধ কি না তা যাচাই করে। এটি খুব দ্রুত কাজ করলেও ডেটার ভেতরের ম্যালওয়্যার শনাক্ত করতে পারে না।

৩) স্টেটফুল ইন্সপেকশন ফায়ারওয়াল (Stateful Inspection Firewall) ঃ এটি প্যাকেট ফিল্টারিং এবং সার্কিট-লেভেল–উভয় প্রযুক্তির সমন্বয়ে কাজ করে। এটি শুধু আইপি চেক করে না, বরং পুরো কানেকশন বা সেশনের ইতিহাস মনে রাখে এবং যাচাই করে যে ট্রাফিকটি কোনো বিশ্বস্ত সূত্র থেকে আসছে কি না।

৪) প্রক্সি ফায়ারওয়াল বা অ্যাপ্লিকেশন ফায়ারওয়াল (Proxy Firewall) ঃ এটি ইন্টারনেটের সাথে সরাসরি সংযোগ হতে দেয় না। হ্যাকার এবং আপনার সিস্টেমের মাঝে এটি একটি "মধ্যস্থতাকারী" (Mediator) হিসেবে কাজ করে। এটি ডেটা প্যাকেটের একদম গভীরে (Application Layer) গিয়ে পরীক্ষা করে।

উদাহরণ ঃ আপনার অফিসের কম্পিউটার থেকে কোনো সাইটে ঢুকলে সেটি আগে প্রক্সি সার্ভারে যায়, তারপর ইন্টারনেটে।

৫) নেক্সট-জেনারেশন ফায়ারওয়াল (Next-Generation Firewall - NGFW) ঃ এটি বর্তমানে সবচেয়ে শক্তিশালী ফায়ারওয়াল। এতে

সাধারণ ফায়ারওয়ালের সব ফিচারের পাশাপাশি IPS (Intrusion Prevention Szstem) এবং Deep Packet Inspection (DPI) করার ক্ষমতা থাকে। এটি আধুনিক এবং জটিল সাইবার হামলা রুখতে সক্ষম।

***** ২। "বিভিন্ন লেয়ারে সাইবার আক্রমণ ঘটতে পারে"- এর যথার্থতা ব্যাখ্যা কর।** বাকাশিবো- ২০২৫

উত্তর ঃ সাইবার নিরাপত্তার ক্ষেত্রে আমরা সাধারণত OSI Model (Open Systems Interconnection Model) অনুসরণ করি, যার ৭টি লেয়ার বা স্তর রয়েছে। হ্যাকাররা তাদের লক্ষ্য অনুযায়ী এই সাতটি স্তরের যেকোনোটিতে আক্রমণ চালাতে পারে।

নিচে বিভিন্ন লেয়ারে সাইবার আক্রমণের উদাহরণসহ যথার্থতা ব্যাখ্যা করা হলো ঃ

১. ফিজিক্যাল লেয়ার (Physical Layer - Layer 1) ঃ এটি নেটওয়ার্কের সবচেয়ে নিচের স্তর, যেখানে হার্ডওয়্যার এবং ক্যাবল থাকে। **আক্রমণ ঃ** তার কেটে ফেলা, ডাটা সেন্টার থেকে হার্ডড্রাইভ চুরি করা, বা ডিভাইসে সরাসরি ক্ষতিকারক কোনো চিপ বা ইউএসবি (USB) লাগানো। **প্রভাব ঃ** পুরো সিস্টেম বা নেটওয়ার্ক সংযোগ বিচ্ছিন্ন হয়ে যায়।

২. ডাটা লিংক লেয়ার (Data Link Layer - Layer 2) ঃ এই লেয়ারে ডিভাইসগুলোর মধ্যে সরাসরি সংযোগ থাকে (যেমনঃ সুইচ বা ওয়াইফাই)। **আক্রমণ ঃ** MAC Spoofing ev ARP Poisoning।

এর মাধ্যমে হ্যাকার নিজেকে বৈধ ইউজার হিসেবে নেটওয়ার্কে তুলে ধরে তথ্য চুরি করে।

৩. নেটওয়ার্ক লেয়ার (Network Layer - Layer 3) ঃ এই স্তরে আইপি (IP) অ্যাড্রেস এবং রাউটিং কাজ করে।

আক্রমণ ঃ IP Spoofing ev ICMP Flood। হ্যাকাররা আইপি অ্যাড্রেস জাল করে ভুল তথ্য পাঠায় বা নেটওয়ার্ক ট্রাফিক জ্যাম করে দেয়।

উদাহরণ ঃ কোনো নির্দিষ্ট আইপি ব্যবহার করে সার্ভার ডাউন করা।

৪. ট্রান্সপোর্ট লেয়ার (Transport Layer - Layer 4) ঃ এই লেয়ারটি ডেটা আদান-প্রদানের নির্ভরযোগ্যতা নিশ্চিত করে (TCP/UDP)।

আক্রমণ ঃ SYN Flood ev TCP Hijacking। হ্যাকাররা অসংখ্য ফেক রিকোয়েস্ট পাঠিয়ে সার্ভারের কানেকশন জ্যাম করে দেয়, যা DoS/DDoS আক্রমণের অংশ।

৫. সেশন লেয়ার (Session Layer - Layer 5) ঃ এই স্তরটি দুই ডিভাইসের মধ্যে সংযোগ বা সেশন তৈরি এবং নিয়ন্ত্রণ করে।

আক্রমণঃ Session Hijacking। আপনার অনলাইন ব্যাংকিং বা ফেসবুক লগইন থাকা অবস্থায় হ্যাকার যদি আপনার "সেশন আইডি" চুরি করে নেয়, তবে সে আপনার পাসওয়ার্ড ছাড়াই অ্যাকাউন্টে ঢুকে পড়তে পারে।

৬. প্রেজেন্টেশন লেয়ার (Presentation Layer - Layer 6) ঃ এটি ডেটাকে এনক্রিপশন বা ডিক্রিপশন করার কাজ করে।

আক্রমণ ঃ Encryption Attack বা ম্যালওয়্যারের মাধ্যমে এনক্রিপশন প্রোটোকল ভেঙে ফেলা। এর ফলে হ্যাকার আপনার গোপন তথ্য সাধারণ টেক্সটে রূপান্তর করে পড়ে নিতে পারে।

৭. অ্যাপ্লিকেশন লেয়ার (Application Layer - Layer 7) ঃ এটি ব্যবহারকারীর সবচেয়ে কাছাকাছি স্তর (যেমনঃ ক্রোম ব্রাউজার, ইমেইল বা ফেসবুক অ্যাপ)। বর্তমানে সবচেয়ে বেশি আক্রমণ এখানেই ঘটে।

আক্রমণ ঃ SQL Injection, Cross-Site Scripting (XSS), Ges Phishing.

প্রভাব ঃ হ্যাকার সরাসরি ডেটাবেস থেকে তথ্য নিয়ে নিতে পারে বা ম্যালওয়্যার ছড়িয়ে দিতে পারে