ইথিক্যাল হ্যাকিং ফ্রী কোর্সঃ- (পর্ব -০১)

বিগেনার টু এক্সপার্ট! কম্পিউটারের প্রতি ভালোবাসা বাড়ছে মানুষের দিনের পর দিন।শুধু ভালোবাসা নয়,কম্পিউটার আরো এবং আরো প্রয়োজনীয় বিষয় হয়ে উঠছে ধীরে ধীরে।কিন্তু কোন জিনিষ থেকে শুধু সুবিধায় পাওয়া যাবে,সেখানে কোন সমস্যাই হবে না,এমন তো হতে পারে না, তাই না? তাই সাইবার ক্রাইম, ব্ল্যাক হ্যাট হ্যাকিং,
ডিডঅ্যাটাক,র‍্যানসমওয়্যার,ম্যালওয়্যার ইত্যাদি বিষয় গুলোও কম্পিউটিং জগতে আগের চেয়ে অনেক বেশি বিস্তার লাভ করেছে। যেমন সমাজে অপরাধ বেড়ে গেলে সমাজ শাসকের প্রয়োজন হয়, ঠিক তেমনি সাইবার ওয়ার্ল্ডে প্রয়োজনীয় হয় সিকিউরিটি স্পেশালিষ্ট বা এথিক্যাল হ্যাকারদের। সবচাইতে ভালো কথা হলো এটা যে, আপনাকে একজন এথিক্যাল হ্যাকার হয়ে উঠতে স্কুল কলেজের মতো বছরের পর বছর ধরে পড়াশুনা করে তারপর যোগ্যতা বা জীবিকার জন্য চিন্তা করতে হবে না। সঠিক জ্ঞান আর প্রশিক্ষণ গ্রহন করার মাধ্যমে আপনি খুব অল্প সময়ের মধ্যেই একজন দক্ষ এথিক্যাল হ্যাকার হিসেবে নিজেকে গড়ে তুলতে পারবেন।

স্কুলের প্রথম দিনে প্রথম ক্লাসে যেমন নাম আর পরিচয় জানতেই দিন শেষ হয়ে যায়, আজকের আর্টিকেলও ঠিক তেমনি শেষ হবে। আমি বছর ০২ আগে যখন প্রথম সাইবার সিকিউরিটি নিয়ে পোস্ট করেছিলাম, সেখানে উল্লেখ্য করেছিলাম এথিক্যাল হ্যাকিং সম্পর্কে, আর তখন থেকেই আপনাদের মাঝে অনেক আগ্রহ লক্ষ্য করেছি। তাই শেষমেষ সম্পূর্ণ কোর্স রিলিজ করবো হিসেবে সিদ্ধান্ত নিয়েছি, আর দেখুন আজ সেই সিদ্ধান্তের ১ম ক্লাস! অনেকেই হ্যাকার হতে চায়, খুব ভালো কথা—কিন্তু হ্যাকিং শেখার আগে অবশ্যই এথিক্যাল হ্যাকিং বিষয়টির উপর আপনার ভালো ধারণা থাকা প্রয়োজনীয়। আমি নৈতিক হ্যাকিং বিষয়টি বুঝাতে অনেকগুলি পোস্ট পূর্বেই গ্রুপে প্রকাশ করেছি, সেইগুলি সর্ব প্রথম পড়ে নেওয়ার জন্য অনুরোধ করবো। যাই হোক, এই সূচনা পর্বে আমি আলোচনা করবো এই সম্পূর্ণ ফ্রী কোর্সে আমরা কি কি শিখতে চলেছি, এবং আমাদের লক্ষ্য আসলে কি হবে।

এথিক্যাল হ্যাকিং ফ্রী কোর্স

আপনি যদি যথেষ্ট সময় এই গ্রুপ বা পেজের সাথে সম্পৃক্ত থাকেন, তবে অবশ্যই জানেন যে, সবুজ বাংলা ইউটিউব হেল্প লাইন এবং সবুজ বাংলা টিভি

কখনোই কোন নলেজ শেয়ার করার জন্য অর্থের ডিম্যান্ড করে নি, আর ভবিষ্যতেও করবে না। আর যদি বলি আমার কথা, সেক্ষেত্রে আমি জ্ঞান শেয়ার করতে ভালোবাসি, আর অবশ্যই কোয়ালিটি কনটেন্ট তৈরি করতেও ভালোবাসি। আমি কোন সার্টিফাইড এথিক্যাল হ্যাকার নই, হ্যাকিং প্র্যাকটিস করি ২০১০ সালের দিক থেকে। আজ পর্যন্ত যা কিছু শিখেছি সব কিছুই অনলাইনের সাহায্য নিয়ে, কখনো কোন পেইড কোর্সও জয়েন করিনি। আসলে, আপনার যদি বেসিক গুলো জানা থাকে, সেই ক্ষেত্রে ওপেন ওয়েবেই এতো বেশিকিছু পেয়ে যাবেন, আপনার পেইড কোর্স জয়েন করার প্রয়োজন পড়বে না, তবে সার্টিফিকেটের জন্য পেইড কোর্স প্রয়োজনীয় হতে পারে। এই ফ্রী এথিক্যাল হ্যাকিং কোর্সে আমি বিগেনার থেকে গীক টাইপ পর্যন্ত এক একটি বিষয় পর্ব আকারে পোস্ট করতেই থাকবো। আসলে নলেজ অর্জন করার কোন শেষ নেই, তাই এই কোর্স কবে শেষ হবে সেটারও কোন নিশ্চয়তা নেই, প্রতিনিয়ত এখানে পর্ব গুলো পোস্ট করেই যাবো। আর হ্যাঁ, এই কোর্সে যতো কিছু শেখানো হবে, সেটা অবশ্যই আগে থেকেই ইন্টারনেটে মজুদ রয়েছে, তবে ইন্টারনেট থেকে সরাসরি শিখতে গেলে আপনি এলোমেলো হয়ে যাবেন। আমি সবকিছু স্টেপ-বাই-স্টেপ গুছিয়ে এখানে বর্ণনা করবো। তবে কোন পেইড কোর্সে সাথে এই ফ্রী কোর্সটিকে তুলনা করবেন না, পেইড কোর্সে অনেক বড় বড় স্পেশালিষ্ট এবং এক্সপার্ট দ্বারা ট্রেইন করা হয়, আমি কোন এক্সপার্ট নয়, তবে যতোটুকু জ্ঞান আমার মধ্যে রয়েছে, আমি সবটুকুই এই কোর্সে ঢেলে দেওয়ার চেস্টা করবো। তো চলুন, এবার জেনে নেওয়া যাক, এই এথিক্যাল হ্যাকিং ফ্রী কোর্স থেকে আপনারা আসলে কি কি শিখতে চলেছেন...

কি কি থাকছে এই ফ্রী কোর্সে?

ওয়েবসাইট হ্যাকিং— ইন্টারনেটে তথ্য সংরক্ষিত থাকার সবচাইতে বিশাল বড় সিন্দুক হচ্ছে বিভিন্ন ওয়েবসাইট গুলো। হাইলি ট্র্যাফিক, হিউজ ডাটাবেজ সমৃদ্ধ ওয়েবসাইট গুলো সহজেই ব্ল্যাক হ্যাটদের টার্গেট হয়ে যেতে পারে। আর ওয়েবসাইট বলতেই কিন্তু ওয়েবসাইট নয়। আজকের দিনে না জানি ততো প্রকারের ল্যাংগুয়েজ আর কতো প্রকারের স্ক্রিপ্ট ব্যবহার করে ওয়েবসাইট গুলোকে তৈরি করা হয়। আজকের সবচাইতে জনপ্রিয় ওয়েবসাইট তৈরির প্ল্যাটফর্ম হচ্ছে সিএমএস গুলো, যেমন ওয়ার্ডপ্রেস, জুমলা ইত্যাদি। আর এই সিএমএস গুলো ব্যবহার করে তৈরি করা ওয়েবসাইট গুলোর ত্রুটির শেষ নেই। এই কোর্সে আমরা বিভিন্ন টাইপের ওয়েবসাইটের ত্রুটি গুলোকে খুঁজে পাওয়ার

পদ্ধতি গুলো আয়ত্ত করবো এবং ত্রুটি গুলোর প্যাচ ফিক্স করা শিখবো। সাথে কোন ওয়েবসাইট'কে টার্গেট করে কিভাবে তার উপর কেস স্ট্যাডি করতে হয় সে ব্যাপার গুলো সম্পর্কেও বিস্তারিত জানবো। কোর্সে আমি সহজ ব্যাপার গুলোকেও বারবার আলোচনা করার চেষ্টা করবো, হয়তো তার জন্য যারা সেগুলো আগে থেকেই জানেন, তারা বিরক্ত হতে পারেন, কিন্তু এখানে আমাকে আমার গ্রুপের এবং পেজের সকল সদস্যদের কথা চিন্তা করতে হবে।

হাতে কলমে হ্যাকিং অ্যান্ড সিকিউরিটি টেস্টিং— যে পর্বে সরাসরি প্র্যাক্টিক্যাল হ্যাকিং দেখানো প্রয়োজন পড়বে সেগুলো স্ক্রীনশট বা ভিডিও তৈরি করে হাতে কলমে দেখানো হবে। এই ফ্রী হ্যাকিং কোর্সে আমি থিয়োরি একটু কমই বোঝাবো, প্রাক্টিক্যাল বেশি দেখাবো। অনেক অনলাইন ফ্রী এথিক্যাল হ্যাকিং কোর্সে দেখা যায় শুধু থিয়োরি বুঝিয়েই কোর্স শেষ করে দেয়, বাট এখানে সেটা করা হবে না। আমি আগে থেকেই অনেক বেসিক নলেজ এখানে মানে সবুজ বাংলা ইউটিউব হেল্পলাইন গ্রুপে এবং আমার পেজে শেয়ার করে রেখেছি, যদি আপনি কিছুই না জানেন, সেক্ষেত্রে সেগুলো আগে পড়ে নিন। প্রয়োজনে অবশ্যই বেসিক বিষয় গুলোর উপর আলোকপাত করা হবে, কিন্তু প্রাক্টিক্যাল'কে বেশি প্রাধান্য দেওয়া হবে।

কালি লিনাক্স (এ-জেড)—

কথা বলা হবে হ্যাকিং নিয়ে আর কালি লিনাক্সের প্রশ্ন আসবে না, সেটা কি হতে পারে? আপনার যদি সাইবার সিকিউরিটি স্পেশালিষ্ট হওয়ার চিন্তা ভাবনা থাকে আর আপনি যদি এই চিন্তার সাথে অত্যন্ত সিরিয়াস হোন, অবশ্যই আপনাকে কালি লিনাক্স এ-জেড পর্যন্ত আয়ত্ত করতে হবে। এই অপারেটিং সিস্টেমটি বিশেষভাবে সাইবার সিকিউরিটি প্রদান করার জন্যই ডিজাইন করা হয়েছে। এই নিয়ে এখানে আর বেশি কিছু বলবো না, তবে এতোটুকু বলে রাখছি, কালি লিনাক্স ছাড়া কখনোই হ্যাকার বলে নিজেকে পরিচিতি দেওয়া আপনার উচিৎ হবে না। ফ্রী কোর্স হয়েছে তো কি হয়েছে, কালি সম্পর্কে এ-জেড নলেজ থাকবে এখানে!

সোশ্যাল ইঞ্জিনিয়ারিং

— এই লাইন বহুবার উল্লেখ্য করেছি বিভিন্ন আর্টিকেলে, "কম্পিউটারের চাইতে মানুষকে হ্যাক করা অনেক বেশি সহজ" আর সোশ্যাল ইঞ্জিনিয়ারিং বলতে

মানুষের মস্তিষ্ক'কে হ্যাক করা বুঝানো হয়। অনেক হ্যাক অ্যাটাক কখনোই সম্ভব হতো না যদি সেখানে সোশ্যাল ইঞ্জিনিয়ারিং এর সাহায্য না নেওয়া হতো। বিশাল বড় সিস্টেম সেটআপ করে আর বহু লাইনের কোডিং করার পরেও একটি সিস্টেম হ্যাক করা ততোটা সহজ হয়না, যতোটা সহজে কাউকে বোকা বানিয়ে পাসওয়ার্ড হাতানো যায়। সোশ্যাল ইঞ্জিনিয়ারিং এর প্রথম পর্যায় থেকে এখানে ইন্টারমিডিয়েট পর্যায় পর্যন্ত আলোচনা করার চেষ্টা করা হবে। যদিও আমি সোশ্যাল ইঞ্জিনিয়ারিং এক্সপার্ট নয়, কিন্তু তারপরেও চেষ্টা করবো কিছু আর্টিকেল সোশ্যাল ইঞ্জিনিয়ারিং এক্সপার্ট দ্বারা লিখিয়ে নেওয়ার।

কমপ্লিট নেটওয়ার্ক টেস্টিং অ্যান্ড হ্যাকিং

— হ্যাকিং আর নেটওয়ার্কিং এক মায়ের পেটের দুই ভাই। আপনি নেটওয়ার্কিং এ যতো বেশি পারদর্শী হবেন, হ্যাকিং আপনার জন্য ততো সহজ ব্যাপার হয়ে উঠবে। নেটওয়ার্কিং এর প্রত্যেকটি কোনা এখানে কভার করার চেষ্টা করবো, অন্তত প্রয়োজনীয় বিষয় গুলো। আমরা যেকোনো নেটওয়ার্ক সিকিউরিটি টেস্টিং সম্পর্কে শিখবো, ত্রুটি খুঁজে বেড় করবো, নেটওয়ার্ক অ্যাক্সেস গ্রহন করতে জানবো। এই কোর্সে ত্রুটি পূর্ণ নেটওয়ার্ক বাইপাস করার কমপ্লিট গাইড শেয়ার করা হবে, সাথে অবশ্যই ত্রুটি ফিক্স করার প্রসঙ্গেও বিস্তারিত আলোচনা করা হবে। ফায়ারওয়াল টেস্টিং থেকে শুরু করে, প্যাকেট ক্যাপচারিং, প্যাকেট এনালাইসিস, ওয়াইফাই টেস্টিং কোন কিছুই বাদ যাবে না এই কোর্সে।

ক্রিপটোগ্রাফি— অনলাইনে ডাটা সিউকিউর করার জন্য এনক্রিপশনের কোন তুলনা হয়না। ক্রিপটোগ্রাফি এমন এক টেকনিক যেটা সাধারণ পড়ার যোগ্য ভাষাকে পরিবর্তন করে পড়ার অসম্ভব করে তোলা হয়। যেহেতু ক্রিপটোগ্রাফি আমাদের প্রয়োজনীয় ডাটা গুলোকে সিকিউরিটি প্রদান করে, তবে অবশ্যই ক্রিপটোগ্রাফি'তে দুর্বলতা থাকলে সেটা সম্পূর্ণ ডাটাকেই ত্রুটিপূর্ণ করে দিতে পারে। এই কোর্সের সবচাইতে অ্যাডভানস লেভেলের আর্টিকেল গুলো হবে এই ক্রিপটোগ্রাফির উপরে। আমরা এনক্রিপশনের মধ্যের ত্রুটি খুঁজে পাওয়া সম্পর্কে জানবো এবং এনক্রিপশনকে আরো মজবুদ করার পদ্ধতি গুলো রপ্ত করবো। এই এথিক্যাল হ্যাকিং ফ্রী কোর্স এ সকল বহুল ব্যবহৃত এনক্রিপশন ম্যাথড গুলো যেমন- AES(Advanced Entyption Standard), DES(Data Encryption Standard), RSA(Name of the creators), MD5(Message Digest -5), SHA(Secure Hash Algorithm), SSL (Secure Socket Layer) —নিয়ে

বিস্তারিত আলোচনা করা হবে।

হ্যাকিং উইথ অ্যান্ড্রয়েড

— আপনার অ্যান্ড্রয়েড মোবাইলটিকে কিন্তু যেমন তেমন ভাববেন না, যদি আপনার কাছে কোন কম্পিউটার না থাকে এই মুহূর্তে, অবশ্যই আপনি অ্যান্ড্রয়েড ফোন বা ট্যাবলেট ব্যবহার করেও অনেক কিছু শিখতে পারবেন। এই কোর্সে আপনার অ্যান্ড্রয়েড ডিভাইজটিকে একটি কমপ্লিট হ্যাকিং মেশিনে তৈরি করেই ছাড়বো। সাথে রাসবেরি পাই ব্যবহার করে হ্যাকিং করা নিয়েও আলোচনা করবো।

প্রোগ্রামিং (বেসিক)

— প্রোগ্রামিং এ ভালো আয়ত্ত থাকা অবশ্যই আপনার জন্য প্লাস পয়েন্ট। যেহেতু আমি নিজেই ভালো প্রোগ্রামার নই, তাই অ্যাডভানস প্রোগ্রামিং এখানে শেয়ার করতে পারব না। তবে বেসিক সবকিছু নিয়েই এখানে আলোচনা করে পোস্ট থাকবে। বিশেষ করে এখানে পাইথনের উপর বেশি জোর দেওয়া হবে।

ডাটাবেজ টেস্টিং অ্যান্ড হ্যাকিং

— বর্তমানে অনেক কোম্পানি তাদের ডাটাবেজ'কে লোকাল কম্পিউটারে ইন্সটল করে রাখে, অথবা ইন্টারনেট সার্ভার থেকে ডাটাবেজ অ্যাক্সেস করে। আর হ্যাকার বড় ধরণের অ্যাটাক চালানোর জন্য প্রথমে ডাটাবেজ'কেই টার্গেট করে। ডাটাবেজে থাকা ত্রুটি সম্পূর্ণ ডাটাবেজটির তথ্য গুলোকে লিক করে দিতে পারে, তাই ডাটাবেজ টেস্টিং এবং ডাটাবেজ ত্রুটি প্যাচ করা সম্পর্কে আপনার বিস্তারিত জ্ঞান থাকা প্রয়োজনীয়। এই কোর্সে আমরা MySQL এবং Oracle ডাটাবেজের সিকিউরিটি চেকিং শিখবো, সাথে ডাটাবেজ অ্যাটাক, ডাটাবেজ ডাটা কালেকশন, ওয়েব নির্ভর ডাটাবেজ সিকিউরিটি নিয়ে বিস্তারিত আলোচনা করবো।

আপনার প্রতি কিছু কথা

আপনি এই পোস্টটি পড়ছেন এবং সামনের পর্ব গুলোর জন্য উৎসাহিত হয়ে

রয়েছেন, খুব ভালো কথা। কিন্তু আমি বা অন্য কোন হাজার ডলারের পেইড কোর্স কখনোই আপনাকে ভালো হ্যাকার/সিকিউরিটি স্পেশালিষ্ট বানাতে পারবে না, যতক্ষণ না পর্যন্ত আপনি নিজে থেকে চেস্টা করবেন। আপনাকে সকল বিষয় গুলো সঠিক অনুশীলন করতে হবে। সাথে বলে রাখি, আপনি যদি অলরেডি অনেক কিছু জানেন বা হ্যাকিং এর যেকোনো একটি বিষয় সম্পর্কে আপনার ভালো আয়ত্ত থাকে, সেক্ষেত্রে এই কোর্সকে এগিয়ে নিয়ে যাওয়ার জন্য সবুজ বাংলা ইউটিউব হেল্পলাইন কে সাহায্য করুণ। এথিক্যাল হ্যাকিং এর এতো বিশাল কোর্স আমার একার দ্বারা কভার করা একটু বেশিই কস্টকর, সাথে অনেক পরিশ্রমের কাজ। যদিও আমি পরিশ্রম করতে বা কাজ করতে ভয় পাই না। কিন্তু তারপরেও আপনার সাহায্য এই কোর্সকে সামনের দিকে এগিয়ে নিয়ে যাবে। আপনার এই কোর্সের সাথে কাজ করার ইচ্ছা এবং ক্ষমতা থাকলে অবশ্যই আমাকে মেইল করুন:- ssobuz2018@gmail.com এই ঠিকানায়।

আর এই কোর্সের কোন হ্যাকিং টেকনিক ব্ল্যাক হ্যাট কাজে ব্যবহার করা যাবে না। ওয়েবসাইট, ডাটাবেজ, মোবাইল অপারেটিং সিস্টেম হ্যাক, কম্পিউটার অ্যাক্সেস ইত্যাদি হ্যাকিং এর জন্য আমি নিজেই ওয়েবসাইট বা ডাটাবেজ প্রদান করবো, যেখানে আপনি টেস্টিং করতে পারবেন। কিন্তু অন্যের ওয়েবসাইটের উপর হ্যাক অ্যাটাক চালানো যাবে না। এথিক্যাল হ্যাকিং এর মূল মন্ত্র ভুলে গেলে কখনোই চলবে না, অবশ্যই আপনাকে সর্বদা ১০০% সৎ থাকতে হবে। আর যদি আপনি কোন অসৎ উদ্দেশ্যে এই কোর্সের শেখানো হ্যাকিং ম্যাথড গুলোকে ব্যবহার করেন, সেই ক্ষেত্রে তার দ্বায়ভার শুধু আপনার হবে। আমি সবুজ কোন ভাবেই নেব না।

আমি এতো কষ্ট করে সকল কোর্স ফ্রী'তে পাবলিশ করবো আর আপনি কিছুই করবেন না, সেটা হলে কিন্তু চলবে না। অবশ্যই আপনাকেও এখানে কিছু করতে হবে, আমাদের সকলের জন্য করতে হবে। অবশ্যই আপনাকে কোর্সের পোস্ট গুলো যতোটা সম্ভব শেয়ার করতে হবে। আমি যতো ভালো রেসপন্স পাবো আপনাদের কাছ থেকে ততো দ্রুত সব পর্ব গুলো পাবলিশ করবো। আমার অনুপ্রেরণা হলেন আপনারা। আর আমাকে অনুপ্রেরণা জোগানর দায়িত্ব আপনাদের।

তো ব্যাস এই ছিল আজকের সূচনা পর্ব, আপনি নিশ্চয় পরিষ্কার ধারণা পেয়ে গেলেন আমরা কি কি বিষয়ের উপর বিস্তারিত জ্ঞান পেতে চলেছি। এটা একটি পাবলিক গ্রুপ, তাই অবশ্যই আপনার মনে যেকোনো প্রশ্ন এখানে মন খুলে প্রকাশ করার সুবিধা রয়েছে। অবশ্যই আপনার যেকোনো মতামত আমাদের সাথে শেয়ার করুণ। আর হ্যাঁ, আমি সপ্তাহে কয়দিন কোর্সের পোস্ট পাবলিশ করবো এই ব্যাপারে আপনাদের মতামত জানান। তবে আমি চেষ্টা করবো অন্তত সপ্তাহে ০৩টি পর্ব প্রকাশ করার। আর আগামীকাল কোর্সের ০২য় পর্ব প্রকাশ করা হবে, তাই সর্বদা সাথেই থাকুন! ধন্যবাদ!

নেটওয়ার্কিং নিয়ে সবকিছু! (বেসিক-১)কল্পনা করুণ, আপনি যদি এই দুনিয়াতে একমাত্র ব্যাক্তি হতেন তাহলে কি আপনাকে কোন কিছু নিয়ে টেনশন করতে হতো? আপনার কোন কিছু হারানোর ভয় থাকতো না, কোন কিছু পাওয়ার আকাঙ্ক্ষা থাকতো না, কোন লোভ, লালসা, আর অস্থিরতাও থাকতো না। সর্বদা হয়তো সৃষ্টিকর্তার প্রতি সন্তুষ্ট থাকতেন, এতো কিছু আপনাকে উপহার দেওয়ার জন্য! ঠিক কম্পিউটিং ওয়ার্ল্ডে যদি “নেটওয়ার্কিং” টার্মটি না থাকতো, আজকের অনেক মডার্ন কম্পিউটিং টেক কল্পনাও করা যেতো না, যেমন- ইন্টারনেট! একসাথে অনেক কম্পিউটার যুক্ত হওয়ার জন্যই যতোসব সমস্যার শুরু, এর ফলেই খারাপ লোকেরা আপনার সিকিউরিটি ব্রেক করার চেষ্টা করবে, আর সিকিউরিটি স্পেশালিষ্ট অত্যন্ত প্রয়োজনীয় হয়ে পড়বে। নেটওয়ার্কিং টার্মটি না থাকলে, আজকের এই হ্যাকিং টার্মটিও হয়তো শুনতে পারতেন না। যেমনটা উপরের উদাহরণ থেকে বুঝতে পারেন, এক সাথে পৃথিবীতে বহু মানুষ রয়েছে বলেই এতো প্রতিযোগিতা, এতো হিংসা বিদ্বেষ।

এথিক্যাল হ্যাকিং ফ্রী কোর্স এর দ্বিতীয় পর্ব একটু দেরিতে পাবলিশ করার জন্য ক্ষমা চেয়ে নিচ্ছি। আসলে যখন কোন কোর্স পাবলিশ করার চেষ্টা করা হয়, সেক্ষেত্রে এটা খুব একটা মুশকিলের কাজ নয়, আপনাকে কোন টপিক কিভাবে বুঝানো হবে—বরং মুশকিলের কাজ হচ্ছে কোন টপিকের পর কোন টপিক বোঝানো হবে। অর্থাৎ বলতে পারেন সূচি পত্র, আর কম্পিউটিং আর হ্যাকিং লাইনের সূচি বানানো একটু মুশকিলের, আপনি যদি এই কাজ আগে না করে থাকেন, তো যতো বড়ই এক্সপার্ট হোন না কেন, আপনার বিষয় গুলো গুছিয়ে নিতে একটু কষ্ট করতে হবে! তো আমার ক্ষেত্রেও হয়েছে তাই, আমি ঠিক করতেই পারছিলাম না, কোন টপিকের পর কোন টপিক শুরু করবো, কেনোনা

প্র্যাক্টিক্যালি এই বিষয় এতোটা সুবিশাল যে সুগঠিত সূচি তৈরি করাটা একটু মুশকিলের। যাই হোক, একেবারে গোঁড়া থেকে শুরু করতে যাচ্ছি, আর তা হলো নেটওয়ার্কিং। তবে আমি সম্পূর্ণ কোর্সটিকে একটু আলাদাভাবে সাজাতে চেষ্টা করবো। যখন নেটওয়ার্কিং নিয়ে আলোচনা করছি, এর মানে এই নয় শুধু নেটওয়ার্কিং নিয়েই সিরিয়াল পর্ব প্রকাশ করেই যাবো! নেটওয়ার্ক নিয়ে আলোচনা করতে করতে হয়তো ওয়াইফাই এর দিয়ে চলে যাবো, তারপরে হয়তো ওয়াইফাই সিকিউরিটি টেস্টিং এর দিকে চলে যাবো, আবার নেটওয়ার্কিং এর আলাদা টার্মে চলে যাবো, তারপরে হয়তো ওয়েব সার্ভার রিলেটেড বিষয়ের দিকে চলে যাবো। সম্পূর্ণ কোর্সটিকে এমনভাবে নিয়ন্ত্রন করবো যাতে আপনারা কখনোই আকর্ষণ হারিয়ে না ফেলেন! কেনো না আমি বিশ্বাস করি সবকিছুতেই বিদ্যা! তো, আশা করছি কোর্সের সামনের পর্ব গুলো সম্পর্কে আপনার মোটামুটি ধারণা হয়ে গিয়েছে! এবার আর একটিও অপ্রয়োজনীয় কথা ছাড়া, সরাসরি নেটওয়ার্কিং এর ভেতরে প্রবেশ করা যাক।

(কম্পিউটার নেটওয়ার্ক)

যখন একাধিক কম্পিউটার একসাথে একই প্রোটোকলে যুক্ত হয়ে কাজ করতে শুরু করে, সহজ ভাষায় একে সাধারণ কম্পিউটার নেটওয়ার্ক বলা হয়। আপনি যখনই একটি কম্পিউটারের সাথে আরেকটি কম্পিউটার যুক্ত করানোর চেষ্টা করবেন, বা কথা বলানোর চেষ্টা করবেন, অবশ্যই আপনাকে নেটওয়ার্ক তৈরি করতে হবে। আপনি ব্লুটুথ ব্যবহার করে এক ফোন থেকে আরেক ফোনে ফাইল বা গান ট্র্যান্সফার করার সময়ও নেটওয়ার্কিংই করে থাকেন। তো এটা একেবারেই বোঝা জলের মতো সহজ, একাধিক কম্পিউটার একই জালে যোগ করে দেওয়ার মাধ্যমেই নেটওয়ার্কিং এর জন্ম হয়। তবে এখানে কিছু গভীর লক্ষণীয় বিষয় রয়েছে। চিন্তা করে দেখুন, আপনি যখন একটি কম্পিউটারের সাথে আরেকটি কম্পিউটার যোগ করছেন, সেক্ষেত্রে এখানে আরো কি কি জিনিষ সামনে চলে আসছে! প্রথমত অবশ্যই কম্পিউটার নিজেই একটি টার্ম, তারপরে কিভাবে এদের নিজেদের মধ্যে কানেক্ট করানো হচ্ছে। যদি তারের মাধ্যমে কানেক্ট করানো হয়, সেক্ষেত্রে ওয়্যার নির্ভর নেটওয়ার্ক আর যদি বিনা তারে কানেক্ট করানো হয়, সেক্ষেত্রে ওয়্যারলেস নেটওয়ার্ক। দুইটি কম্পিউটার হয়তো অনেক সহজেই ডাইরেক্ট কানেকশন তৈরি করে একে ওপরের সাথে কানেক্টেড করাতে পারবেন, কিন্তু যদি কম্পিউটারের সংখ্যা বাড়িয়ে দেওয়া হয়, সেক্ষেত্রে অবশ্যই আরেকটি তৃতীয়পক্ষ ডিভাইজের প্রয়োজন পড়বে, যেটা

সকল কানেকশন গুলোকে মেইন্টেইন করবে। যেমন ধরুন সহজেই আপনি একটি বা দুইটি প্লাগ সরাসরি ওয়াল সকেটে কানেক্ট করতে পারবেন, কিন্তু যদি টিভি, ফ্রিজ, মোবাইল, ল্যাপটপ চার্জার, একসাথে কানেক্ট করা প্রয়োজনীয় হয়ে পরে তখন ম্যাল্টি-প্ল্যাগ প্রয়োজনীয় হয়। নেটওয়ার্কিং এর ক্ষেত্রে রাউটার,হাব,এবং সুইচ এই কাজটিই করে থাকে। এবার ব্যাস কম্পিউটার গুলোকে এক কানেকশনে জুড়ে দিলেন, কিন্তু তারপরেও টেকনিক্যালি নেটওয়ার্ক তৈরি হবে না, যতোক্ষণ পর্যন্ত কম্পিউটার গুলো একই প্রোটোকলে কাজ করতে আরম্ভ না করবে, অবশ্যই প্রত্যেক কম্পিউটার'কে প্রত্যেকের ভাষা বুঝতে হবে। ধরুন আমি বাংলা বলি আর আপনি বলেন চাইনিজ, সেক্ষেত্রে কি কখনো আপনার আর আমার মধ্যে কমিউনিকেশন সম্ভব হবে? আরেকটি হার্ডওয়্যার অংশ নেটওয়ার্কিং সম্পূর্ণ করতে সাহায্য করে, সেটা হচ্ছে আপনার কম্পিউটারে থাকা নেটওয়ার্ক কার্ড। পূর্বে এটি আলাদা করে লাগানোর প্রয়োজন পড়ত, কিন্তু বর্তমানে সকল কম্পিউটারের সাথে এটি ডেডিকেটেড ভাবেই লাগানো থাকে।

(আইপি অ্যাড্রেস)

এখন ধরুন, আপনি একাধিক কম্পিউটারকে একত্রে একটি নেটওয়ার্কে জুড়ে দিয়েছেন, কিন্তু কোন নির্দিষ্ট কম্পিউটার কিভাবে কোন নির্দিষ্ট কম্পিউটারের সাথে সম্পর্ক স্থাপন করবে? ধরুন আপনি একটি ম্যাল্টি-প্ল্যাগে ১০টি ইলেকট্রিক ডিভাইজ যুক্ত করে রেখেছেন, এখন যদি এতে কারেন্ট প্রদান করেন তো প্রত্যেকটি ডিভাইজ সমানভাবে কারেন্ট রিসিভ করবে। কিন্তু আপনি যদি নির্দিষ্ট ইলেকট্রিক ডিভাইজকে নির্দিষ্ট কারেন্ট প্রদান করতে চান, সেক্ষেত্রে অবশ্যই কানেক্টেড থাকা ডিভাইজ গুলোর একটি পরিচয় থাকা প্রয়োজনীয়। কম্পিউটার নেটওয়ার্কেও বিষয়টি অনেকটা একই রকম। আইপি অ্যাড্রেস হলো কোন কম্পিউটারের ভার্চুয়াল পরিচয়, যেটার সাহায্যে নেটওয়ার্কে কানেক্টেড থাকা যেকোনো কম্পিউটারকে সহজেই খুঁজে বেড় করা সম্ভব। আইপি অ্যাড্রেস, সাধারণত দেখতে "১৫১.১০১.৬৫.১২১" —এই রকমের হয়ে থাকে। কিন্তু বিভিন্ন টাইপের আইপি অ্যাড্রেস থাকতে পারে। আর টাইপ অনুসারে এর নাম্বারিক পরিবর্তনও হতে পারে। তো আমরা উপরের রেফারেন্স অনুসারে কাজ করবো। প্রথমে আমরা কম্পিউটার গুলোকে একত্রে নেটওয়ার্কের সাথে যুক্ত করেছি এবং এখন আমাদের কাছে সকল কম্পিউটারের ইউনিক পরিচয় রয়েছে, অর্থাৎ যেকোনো স্পেশাল কম্পিউটারে স্পেশাল ডাটা

বা কম্যান্ড সেন্ড করা সম্ভব হবে। এখন অবশ্যই নেটওয়ার্কিং এর দুইটি আলাদা ভাগ রয়েছে। যদি আপনি নিজের বাড়িতে বা অফিসে থাকা কম্পিউটার গুলোকে একসাথে তারের মাধ্যমে কানেক্ট করে বা ওয়্যারলেস ভাবে কানেক্ট করে নেটওয়ার্ক তৈরি করেন, তো সেটা লোকাল নেটওয়ার্ক বলা হবে। যদি আপনার লোকাল নেটওয়ার্ককে বাইরের হাজারো-লাখো লোকাল নেটওয়ার্কের সাথে জুড়ে দেন, তো সেটাকেই ইন্টারনেট বলা হয়। ইন্টারনেট নিয়ে বিস্তারিত। এখানে আর কিছুই বলবো না, অলরেডি গ্রুপে বেস্ট পোস্ট পাবলিশ করে রেখেছি, পড়ে নিতে পারেন। লোকাল নেটওয়ার্ক আর ইন্টারনেট অনেকটা একইভাবেই কাজ করে, কিন্তু জিনিষ আলাদা থাকে। যেমন ধরুন, আপনি যখন বাড়িতে থাকেন, সেখানে আপনি নিজেই বস, কেনোনা আপনার বাড়ি, ঠিক? আবার যখন বাইরে থাকেন, বা অফিসে থাকেন, সেখানে আরেক নিয়মে আপনাকে চলতে হয়, কেনোনা সেখানে বস অন্যকেউ।

(আইপি টাইপ)

উপরে যে আইপি অ্যাড্রেসের বর্ণনা করেছি, সেটা হচ্ছে আইপি ভার্সন ৪ — যেটা অলরেডি শেষ হয়ে গিয়েছে। যখন আপনি ইন্টারনেটে কানেক্টেড থাকবেন, অবশ্যই এর মানে লাখো ডিভাইজের সাথে কানেক্টেড হয়ে গেলেন তাই না। কিন্তু সেখানে তো অবশ্যই ইউনিক অ্যাড্রেস প্রয়োজনীয় হবে, রাইট? ব্যাট ভার্সন ৪ অনেক আগেই শেষ হয়ে গেছে। আমরা এক নেটওয়ার্ক অ্যাড্রেস ট্র্যান্সলেসন পদ্ধতি ব্যবহার করে এই আইপি ৪ এর ঘাটতি পূরণ করছি।গ্রুপে আইপি অ্যাড্রেস নিয়ে ডেডিকেটেড পোস্ট রয়েছে, যেটা দেখে নেওয়া আবশ্যক! আগেই বলেছি, অনেক টাইপের আইপি অ্যাড্রেস রয়েছে, এবং সকলের রুল নেটওয়ার্কিং এর ক্ষেত্রে আলাদা হয়ে থাকে। প্রাইভেট আইপি, পাবলিক আইপি, স্ট্যাটিক আইপি, এবং ডাইন্যামিক আইপি। প্রাইভেট আইপি হলো আপনার লোকাল নেটওয়ার্কের ব্যবহৃত আইপি অ্যাড্রেস। আগেই বলেছি, আইপি ৪ শেষ হয়ে গেছে, কিন্তু প্রাইভেট নেটওয়ার্কে আপনি এমন কোন আইপি যদি ব্যবহার করেন, যেটা আলাদা বা অন্য নেটওয়ার্কে থাকা ডিভাইজেরও রয়েছে, আপনার নেটওয়ার্কের কোন কিছু যায় আসবে না। কেনোনা নিজের নেটওয়ার্ক, নিজের রুলস! ১০.০.০.০ থেকে ১০.২৫৫.২৫৫.২৫৫ , ১৭২.১৬.০.০ থেকে ১৭২.৩১.২৫৫.২৫৫ | এবং ১৯২.১৬৮.০.০ থেকে ১৯২.১৬৮.২৫৫.২৫৫ —এই রেঞ্জের আইপি গুলোকে প্রাইভেট আইপি হিসেবে ব্যবহৃত করা হয়। এখন এর মধে আপনার

কম্পিউটারের প্রাইভেট আইপি হতে পারে “১৯২.১৬৮.০.১০” এইটা কিন্তু ইন্টারনেট আইপি নয়, এটা আপনার নিজস্ব আইপি। এখন ইন্টারনেটের সাথে কানেক্টেড হতে অবশ্যই পাবলিক আইপি প্রয়োজনীয় হবে। পাবলিক আইপি সেই আইপি যেটা ইন্টারনেট সার্ভিস প্রভাইডার আপনাকে প্রদান করে। আপনি কম্পিউটার অন করলেন, আর ইন্টারনেটের সাথে কানেক্টেড হলেন, এর অর্থ কি? এর অর্থ হচ্ছে আপনি আপনার ইন্টারনেট সার্ভিস প্রভাইডারের কম্পিউটার কানেক্ট করলেন, এবং তার কাছ থেকে একটি পাবলিক আইপি গ্রহন করলেন। বন্ধু, এখানেই নেটওয়ার্ক অ্যাড্রেস ট্র্যান্সলেশন বা ন্যাট (NAT) কে কাজে লাগানো হয়। আপনার রাউটার শুধু মাত্র পাবলিক আইপি গ্রহন করে এবং আপনার লোকাল বা হোম নেটওয়ার্কের প্রাইভেট আইপি গুলোকে পেছনে লুকিয়ে রাখে। রাউটার সকল কানেক্টেড থাকা ডিভাইজ গুলোকে একটি প্রাইভেট আইপি প্রদান করে এবং যখন কোন কম্পিউটার থেকে ইন্টারনেটের কাছে রিকোয়েস্ট করা হয়, রাউটার সেই রিকোয়েস্ট গ্রহন করে এবং পাবলিক আইপিতে পাঠিয়ে দেয়। পাবলিক আইপি থেকে ফিরে আশা রিকোয়েস্ট রাউটারের কাছে আসে, রাউটার সেটা আপনার কম্পিউটারের প্রাইভেট আইপিতে পাঠিয়ে দেয়, কেনোনা রাউটার ভালো করেই জানে, কোন প্রাইভেট আইপি থেকে রিকোয়েস্টটি এসেছিলো, এবং কোথায় সেটাকে পাঠাতে হবে! বুঝতে পারলেন তো? এভাবেই ন্যাট ব্যবহার করে ইন্টারনেটকে জীবিত করে রাখা হয়েছে।

(ডাইন্যামিক আইপি) |(স্ট্যাটিক আইপি)

বেশিরভাগ পাবলিক আইপি অ্যাড্রেস পরিবর্তন হতে থাকে। মানে আপনি একবার ইন্টারনেট কানেক্ট করলেন, আপনাকে এক পাবলিক অ্যাড্রেস দেওয়া হলো, কিন্তু ডিস্কানেক্ট করে আবার কানেক্ট করলে আরেক পাবলিক আইপি দেওয়া হয়, বিশেষ করে মোবাইল অপারেটর’রা এই কাজটি বেশি করে থাকে। তো যদি কোন আইপি পরিবর্তন হয়ে যায়, সেক্ষেত্রে সেটাকে ডাইন্যামিক আইপি বলা হয়। ধরুন, আপনি ইন্টারনেট ব্যবহার করছেন না, তারপরেও তো আপনাকে সেই পাবলিক আইপি দিয়ে রাখার কোন দরকার নেই তাই না? এই আইএসপি রা অন্য কাস্টমারকে সেই আইপি দিয়ে দেয়। এমনতিই আইপি অ্যাড্রেসের ঘাটতি রয়েছে, বুঝতেই তো পাড়ছেন! তবে আপনি যদি কোন ওয়েবসাইট হোস্ট করতে চান, সেক্ষেত্রে স্ট্যাটিক আইপি অ্যাড্রেস প্রয়োজনীয় হবে। যদি আইপি পরিবর্তন হতেই থাকে, কেউ আপনার কম্পিউটারের সাথে

যোগাযোগ করতে পারবে না। আর ওয়েবসাইট গুলো আপনার কম্পিউটারের মতোই কম্পিউটারে হোস্ট করা থাকে। আপনার হোম নেটওয়ার্ক যেমন পাবলিক আইপির সাথে কানেক্টেড হয়ে ইন্টারনেট অ্যাক্সেস পায়, ঠিক সার্ভার নেটওয়ার্কও পাবলিক আইপির সাথেই কানেক্টেড হতে হয়। বুঝলেন তো, বিষয়টা আসলে সব জায়গাতেই একই। আপনি যদি নিয়মিত আপনার বাড়িতে কুরিয়ার সার্ভিস রিসিভ করতে চান, তাহলে অবশ্যই একটি নির্দিষ্ট এবং অপরিবর্তনশীল ঠিকানা প্রয়োজনীয় হবে। যদি ঠিকানা চেঞ্জ হতেই থাকে, তো বলুন কিভাবে আপনার বাড়ি বারবার খুঁজে পাওয়া যাবে?

(ডিএনএস)

ওয়েবসাইট গুলোতে সরাসরি আইপি না ব্যবহার করে ডোমেইন নাম (যেমন- sobuzbanglatv.com) ব্যবহার করা হয়, যেটা মনে রাখা অনেক বেশি সহজ এবং এতে অনেক সুবিধাও রয়েছে। কিন্তু আইপি ছাড়া কোন কম্পিউটার কানেক্ট করা সম্ভব নয়। তাই যখন আপনি ডোমাইন নাম ব্রাউজারে প্রবেশ করান, ব্রাউজার ডিএনএস বা ডোমেইন নেম সার্ভারের জন্য খোঁজ করতে আরম্ভ করে। ডিএনএস এ সেই তথ্য থাকে, ঐ ডোমেইনটি কোন আইপিতে টার্গেট করা রয়েছে, এর পরে জাস্ট ঐ আইপি থেকে সাইট লোড করা হয়। দ্য ওয়ার্ল্ড ওয়াইড ওয়েব আর্টিকেলটি থেকে আরো বিস্তারিত জানতে পারবেন এই ব্যাপারে।ডোমেইন নাম থাকার সুবিধা হচ্ছে একে তো এটি মনে রাখতে সহজ এবং ডিএনএস পরিবর্তন করা যায়। মানে আপনি যদি এক সার্ভার থেকে আরেক সার্ভারে সাইট ট্র্যান্সফার করেন, মানে আইপি অ্যাড্রেস পরিবর্তন হয়ে যায় কোন সাইটের সেক্ষেত্রে ডিএনএস পরিবর্তন করে দিলেই হয়, এতে সাইট নাম পরিবর্তন করার দরকার পড়ে না। ইউজার বুঝতেই পারবেনা, সার্ভার পরিবর্তন করা হলো কিনা। কিন্তু আপনার আইএসপি ডিএনএস রেকর্ড আপডেট করতে একটু দেরি করতে পারে, ফলে ডোমেইনের পেছনে আইপি পরিবর্তন হলে সাথে সাথে রেকর্ড থেকে সেই আইপি না পেয়ে আগের আইপি চলে আসে, তাই সাইট ডাউন থাকতে পারে। এজন্যই ওয়্যারবিডি সার্ভার পরিবর্তন করার পরে কিছু সময় আপনারা ঢুকতে পারেন না।

(লোকাল এরিয়া নেটওয়ার্ক) বা (ল্যান)

যদিও উপরের আলোচনা থেকে ল্যান সম্পর্কে আপনার ভালো ধারণা হয়ে গিয়েছে, তারপরেও একটু আলোচনা করে নেওয়া প্রয়োজনীয়! আগেই বলেছি, যে কম্পিউটার গুলো ফিজিক্যালি অনেক কাছে থাকে এবং তার বা ওয়্যারলেসের মাধ্যমে একে অপরের সাথে কানেক্টেড থাকে, সেই নেটওয়ার্ককেই ল্যান বলে। ল্যানের মধ্যে কানেকশন ইথেরনেট ক্যাবল, বা ওয়াইফাই ব্যবহার করে দেওয়া যেতে পারে এবং রাউটার, হ্যাব, সুইচ ইত্যাদি প্রয়োজনীয় হয়। ল্যানে ডিভাইজ গুলো সরাসরি একে অপরের সাথে কানেক্টেড থাকে। যেকোনো ডিভাইজ যেকোনো ডিভাইজের সাথে কানেকশন তৈরি করতে পারে এবং ডাটা সেন্ড বা রিসিভ করতে পারে, যেটাকে peer-to-peer নেটওয়ার্ক বলা হয়, বলতে পারেন যেভাবে টরেন্ট নেটওয়ার্ক কাজ করে। কিন্তু ইন্টারনেটের মতো বড় নেটওয়ার্ক এইভাবে কাজ করে না, সেখানে মধ্য হিসেবে থাকে ওয়েব সার্ভার কম্পিউটার, যেকোনো রিকোয়েস্ট পূর্বে সার্ভারের কাছে যায় তারপরে ক্লায়েন্ট কম্পিউটারের কাছে ফাইল/ওয়েবপেজ যায়। এখন প্রশ্ন হচ্ছে, এই লোকাল এরিয়া নেটওয়ার্ক ঠিক কতোবড় তৈরি করা সম্ভব? দুইটি ডিভাইজ থেকে শুরু করে হাজারো বা লাখো ডিভাইজ দিয়ে লোকাল এরিয়া নেটওয়ার্ক তৈরি করা সম্ভব, কিন্তু লাখো ডিভাইজ থাকার পরেও এটাকে ইন্টারনেট বা যাবে না, এর জন্য আপনাকে বাকী দুনিয়ার নেটওয়ার্কের সাথে যুক্ত হতে হবে। কিন্তু লাখো ডিভাইজের লোকাল নেটওয়ার্ক'কে আপনার নিজস্ব ইন্টারনেট বলতে পারেন।

(ওয়াইড এরিয়া নেটওয়ার্ক এবং অন্যান্য)

আগেই বলেছি, অনেক টাইপের নেটওয়ার্ক রয়েছে এবং প্রত্যেকের ভূমিকা এবং গুরুত্ব আলাদা আলাদা, ওয়াইড এরিয়া নেটওয়ার্ক এদের মধ্যে অন্যতম, ইন্টারনেটকে ওয়্যান (WAN) (ওয়াইড এরিয়া নেটওয়ার্ক) বলতে পারেন। এখানে ওয়্যান বলতে বহু দূরত্বে থাকা কম্পিউটার নেটওয়ার্ক'কে বুঝানো হয়েছে। ইন্টারনেট নেটওয়ার্ক গোটা পৃথিবী জুড়ে বিস্তৃত রয়েছে। নেটওয়ার্ক ডিভাইজ রাউটার, এই ল্যান এবং ওয়্যান কে একসাথে কানেক্টেড করে। মানে আপনি লোকাল নেটওয়ার্ক থেকে যখন ইন্টারনেটে কানেক্ট হোন, এর মানে আপনি ওয়্যানের সাথে কানেকশন তৈরি করেন। কিন্তু ওয়্যানকেউ সম্পূর্ণ ইন্টারনেট বলা যাবে না। ধরুন আপনি একটি ব্যাংক নেটওয়ার্ক তৈরি করেছেন, প্রত্যেকটি

ব্যাংকে একটি করে লোকাল নেটওয়ার্ক রয়েছে এবং ব্যাংকের শাখা শহরের বিভিন্ন প্রান্তে ছড়িয়ে রয়েছে, এখন সকল লোকাল নেটওয়ার্ক গুলোকে যদি কানেক্টেড করিয়ে দেন, এক্ষেত্রে টেকনিক্যালি WAN তৈরি হয়ে যাবে। কিন্তু সেটাকে কতক্ষণ পর্যন্ত ইন্টারনেট বলা যাবে না, যতক্ষণ কোন আইএসপি থেকে কানেকশন নিয়ে এই WAN এ কানেক্টেড করবেন। তো বলতে পারেন, আইএসপি যেকোনো ল্যান বা WAN এ ইন্টারনেট কানেকশন প্রদান করে।

আরো কিছু টাইপের নেটওয়ার্ক রয়েছে, যেমন:- WLAN – Wireless Local Area NetworkMAN – Metropolitan Area NetworkSAN – Storage Area Network, System Area Network, Server Area Network, or sometimes Small Area NetworkCAN – Campus Area Network, Controller Area Network, or sometimes Cluster Area NetworkPAN – Personal Area Network

ওয়্যারলেস লোকাল এরিয়া নেটওয়ার্ক মূলত ওয়াইফাই বা আলাদা ওয়্যারলেস টেকনোলোজির উপর নির্ভরশীল, যে ল্যান ওয়াইফাই দিয়ে কানেক্ট করবেন, তাকে ডাব্লিউ ল্যান বলতে পারেন। মেট্রোপলিটন এরিয়া নেটওয়ার্ক বিভিন্ন স্থানে ছড়িয়ে থাকতে পারে, এটি ল্যান থেকে বড় কিন্তু ওয়্যান থেকে ছোট হয়ে থাকে। ফাইবার চ্যানেল টেকনোলজি ব্যবহার করে ডাটাবেজ বা স্টোরেজ বিশেষ কম্পিউটার গুলো নেটওয়ার্কে কানেক্টেড থাকলে একে স্যান বা স্টোরেজ এরিয়া নেটওয়ার্ক বলা হয়। বড় এবং হাই কনফিগ কম্পিউটার গুলোকে একসাথে নেটওয়ার্কে যুক্ত করার মাধ্যমে ক্লাস্টার এরিয়া নেটওয়ার্ক তৈরি করা যায়। তো এই ছিল দ্বিতীয় পর্বের নেটওয়ার্কিং নিয়ে সবকিছুর বেসিক পার্ট ১ কোর্স। আজকের কোর্স এখানেই শেষ করছি, কেন না, এমনিতেই এই পোস্টটাকে অনেক লম্বা করে ফেলেছি, হয়তো এর মধ্যের অনেক তথ্য আপনার আগেই জানা ছিল, কিন্তু তারপরেও একবার অনুশীলন করে নেওয়া ভালো। নেটওয়ার্কিং পার্ট ২ তে কিছু প্র্যাকটিক্যাল বিষয় দেখানো হবে। যেমন- নিচের নেটওয়ার্ক কার্ডের আইপি খুঁজে পাওয়া, লোকাল আইপি খুঁজে পাওয়া, ডিএনএস টুলের ব্যবহার এবং বিস্তারিত আর প্র্যাকটিক্যাল আলোচনা, সাথে আমরা দেখবো কিভাবে ডাইন্যামিক আইপি থেকে স্ট্যাটিক আইপি বানানো যায়, ম্যাক অ্যাড্রেস নিয়েও বিস্তারিত থাকছে সামনের অংশে! তো দ্বিতীয় পর্বের নেটওয়ার্কিং পার্ট ২ কোর্সের অপেক্ষায় থাকুন, সেখানে অবশ্যই মজার

কিছু শিখতে পাবেন বলে আশা রাখছি! এই পর্বের কোর্স কেমন লাগলো, আমাকে নিচে কমেন্ট করে জানাবেন। কোন প্রশ্ন থাকলে অবশ্যই নিচে উল্লেখ্য করবেন!

ইথিক্যাল হ্যাকিং ফ্রী কোর্সঃ পর্ব-০৩(আইপি অ্যাড্রেস বৃত্তান্ত)ইথিক্যাল হ্যাকিং ফ্রী কোর্স পর্ব গুলো একটু দ্রুত প্রকাশ করলে, জানি সকলের মুখ গুলো খুশিতে উজ্জ্বল হয়ে যায়! আর বিশ্বাস করুণ ভাই এবং বন্ধুরা, আপনাদের আমি এরকমই হ্যাপি আর পরিতৃপ্ত দেখতে চাই! আগের পর্ব ০২ তে বলেছিলাম, নেক্সট পর্বে শুধু বেসিক নয়, বরং সাথে কিছু অ্যাডভান্স বিষয় নিয়েও হাজির হবো, তো ব্যাস হাজির হয়ে গেলাম। যারা এই পর্ব প্রথম পড়ছেন, অবশ্যই আগের আরো দুইটি অসাধারণ পর্ব মিস করে ফেলেছেন, যেগুলোকে এখানো গ্রুপে খুঁজে পাবেন। গেলো গত পর্বে নেটওয়ার্কিং নিয়ে বেসিক বিষয় গুলো আলোচনা করেছিলাম এবং আইপি অ্যাড্রেস সম্পর্কে বেশ একটু ধারণা দিয়েছিলাম, এই পর্বটি শুধু আইপি অ্যাড্রেসের উপরই উৎসর্গ করলাম, কেনোনা নেটওয়ার্কিং এর ক্ষেত্রে এটি বিশাল গুরুত্বপূর্ণ একটি বিষয়।

এই কোর্সে যা যা রয়েছে:- কিভাবে নিজের আইপি অ্যাড্রেস খুঁজে পাবো? কি ভাবে আইপি অ্যাড্রেস পরিবর্তন করবো? যে কোন ওয়েবসাইট এর আইপি এড্রেস কিভাবে খুজে পাবো? ইমেইল থেকে সেন্ডারের আইপি অ্যাড্রেস কিভাবে খুজে পাবো? আইপি অ্যাড্রেস থেকে জিও লোকেশন কি সত্যি খুঁজে পাওয়া সম্ভব?১২৮.০.০.১ আইপি অ্যাড্রেস সম্পর্কে বিস্তারিত? ডায়নামিক হোস্ট কনফিগারেশন প্রটোকল কি? আইপি অ্যাড্রেস ব্যবহার করে কিভাবে ম্যাক এড্রেস খুঁজে বের করবো? ফরওয়ার্ড এবং রিভার্স আইপিএল ডিএনএস লুকআপ কি? এইসব গূরুতপূর্ণ বিষয় নিয়ে,তো বুঝতেই পাড়ছেন, কতো অসাধারণ আর প্রিমিয়াম সব তথ্য দিয়ে ইথিক্যাল হ্যাকিং ফ্রী কোর্স পর্ব ০৩ কে সাজানো হয়েছে! এবার জাস্ট ঠাণ্ডা হয়ে বসুন। আর মনোযোগ সহকারে কোর্সটি উপভোগ করুণ!

(নিজের আইপি অ্যাড্রেস খোঁজা)

আপনার কম্পিউটারটি ইন্টারনেট বা যেকোনো এক্সটারনাল নেটওয়ার্কের সাথে যুক্ত রয়েছে, এর মানে এখানে একসাথে দুইটি আইপি অ্যাড্রেস এর ব্যাপার চলে

আসে। একটি পাবলিক বা এক্সটার্নাল আইপি অ্যাড্রেস, যেটা আপনার আইএসপি আপনাকে প্রদান করেছে এবং আরেকটি প্রাইভেট আইপি অ্যাড্রেস বা লোকাল আইপি অ্যাড্রেস। আগের পর্বে স্পষ্ট করে বর্বণা করেছি, অবশ্যই ইন্টারনেট কানেকশন পেতে, যেকোনো ওয়েবসাইট ভিজিট করতে বা অনলাইন ভিডিও স্ট্রিম করতে অবশ্যই পাবলিক আইপি'র সাথে আপনার কানেক্টেড হওয়া জরুরী। প্রাইভেট আইপি ব্যবহার করে লোকাল নেটওয়ার্কে ফাইল শেয়ারিং, প্রিন্টিং, পোর্ট ফরওয়ার্ডিং, অথবা আপনার রাউটার সেটিং অ্যাক্সেস করতে পারবেন। তো যদি বলা হয়, নিজের আইপি অ্যাড্রেস খুঁজে পাওয়ার কথা সেখানে অবশ্যই পাবলিক আইপিকে প্রথমে বুঝানো হয়, যেটাকে আপনার ইন্টারনেট আইপিও বলতে পারেন। হোম নেটওয়ার্কে শুধু আপনার রাউটারের কাছে পাবলিক আইপি অ্যাড্রেস রয়েছে, বাকী কানেক্টেড থাকা ডিভাইজ গুলোকে রাউটার প্রাইভেট আইপির সাথে কানেক্টেড করে রাখে। যাই হোক, যেকোনো পাবলিক আইপি অ্যাড্রেস খুঁজে পাওয়া অনেক সহজ কাজ। ইন্টারনেটে অনেক ওয়েবসাইট রয়েছে, যেগুলো আপনাকে আপনার পাবলিক আইপি অ্যাড্রেস খুঁজে পেতে সাহায্য করে। জাস্ট নিচের লিস্টে বর্ণিত সাইট গুলো ওপেন করুণ, পেজ খুলতেই আপনার পাবলিক আইপি অ্যাড্রেস দেখতে পাবেন। আরো সহজ পদ্ধতি হচ্ছে, গুগলে গিয়ে "What is my ip" লিখে সার্চ করা! তবে হ্যাঁ, আপনি যদি ভিপিএন ব্যবহার করে থাকেন, তবে এই ওয়েবসাইট গুলো আপনার আসল ইন্টারনেট আইপি প্রদর্শিত করতে পারবে না, বরং ভিপিএন সার্ভার আইপি প্রদর্শিত করবে। যেকোনো প্রক্সি সার্ভার ব্যবহার করলে সেই আইপি প্রদর্শিত হবে। এবার প্রশ্ন হচ্ছে কিভাবে লোকাল আইপি বা প্রাইভেট আইপি খুঁজে বেড় করবেন।দেখুন, উইন্ডোজের সকল মডার্ন ভার্সনে "ipconfig" ইউটিলিটি কম্যান্ড প্রমটে আগে থেকেই জুড়ে দেওয়া থাকে। জাস্ট আপনার উইন্ডোজ সিএমডি ওপেন করুণ। সিএমডি ওপেন করার জন্য, উইন্ডোজ কী চেপে ধরে থেকে "R" চাপুন, এভাবে রান ওপেন হবে। এবার রানের ফাঁকা ঘরে গিয়ে লিখুন "cmd" এবং কিবোর্ড থেকে এন্টার প্রেস করুণ, ব্যাস কম্যান্ড প্রমট ওপেন হয়ে যাবে। এবার কম্যান্ড প্রবেশ করান, "ipconfig", দেখবেন সকল আইপি অ্যাড্রেস গুলো এবং নেটওয়ার্ক হার্ডওয়্যার গুলোর বিস্তারিত শো করবে। আপনি যদি ওয়াইফাই ব্যবহার করে ইন্টারনেট সংযুক্ত করে থাকেন, অবশ্যই "Wireless LAN adapter Wi-Fi" সিলেকশন থেকে আপনার লোকাল আইপি দেখানো হবে। আর যদি আপনি ইথারনেট ব্যবহার করেন সেক্ষেত্রে "Ethernet adapter Local Area Connection." সেকশনে আপনার লোকাল আইপি প্রদর্শিত হবে। লোকাল আইপি দেখতে 192.168.0.0

থেকে 192.168.255.255 এর মধ্যে যেকোনো কিছু হতে পারে।

(আইপি অ্যাড্রেস পরিবর্তন)

অনেক কারণ রয়েছে যার জন্য আইপি অ্যাড্রেস পরিবর্তন করা প্রয়োজনীয় হয়ে উঠতে পারে। অনেকে তাদের পাবলিক আইপি বা ইন্টারনেট আইপি পরিবর্তন করতে পছন্দ করে ব্যান ওয়েবসাইট গুলোকে আনব্লক করতে, কান্ট্রি রেস্ট্রিকশন বাইপাস করতে বা যেকোনো ভিডিও দেখার জন্য। এখানে পাবলিক এবং প্রাইভেট দুই ধরণের আইপি'ই পরিবর্তন করা যায়, আর এদের আলাদা আলাদা সুবিধা রয়েছে। এই পর্বে রাউটার থেকে আইপি পরিবর্তন নিয়ে আলোচনা করবো না, এখানে আলচনা করবো কিভাবে আপনার ইন্টারনেট আইপি অ্যাড্রেস পরিবর্তন করতে হবে। তবে এখানে সাফ সাফ করে বলে রাখছি, আইপি পরিবর্তন করে যেকোনো অসৎ কাজ করার উদ্দেশ্য থেকে বিরত থাকুন। আপনি যে আইপি'ই পরিবর্তন করুণ না কেন, আপনাকে খুঁজে পাওয়া সম্ভব, যখন আপনি কোন ক্রাইম করবেন। আর আমরা যেহেতু এথিক্যাল হ্যাকিং শিখছি, তাই অবশ্যই আমাদের মনকে সবার আগে সৎ বানাতে হবে। পাবলিক আইপি'ই আপনার লোকাল নেটওয়ার্ক এবং আপনার কম্পিউটার বা যেকোনো ডিভাইজের পরিচয় ইন্টারনেটের সামনে তুলে ধরে। যদি পাবলিক আইপি পরিবর্তন করা হয়, সেক্ষেত্রে আপনার লোকেশন, দেশ এগুলো লুকিয়ে যায়। আপনি ভিপিএন বা ভার্চুয়াল প্রাইভেট নেটওয়ার্ক ক্লায়েন্ট ব্যবহার করে পাবলিক আইপি অ্যাড্রেস পরিবর্তন করে ফেলতে পারেন। কোন ভিপিএন ক্লায়েন্ট সফটওয়্যার আপনার সিস্টেমে ইন্সটল করতে হবে যেটা আপনার কম্পিউটার এবং ভিপিএন সার্ভারের মধ্যে একটি ট্যানেল তৈরি করবে। যেকোনো ইন্টারনেট রিকোয়েস্ট তখন আপনার আইএসপি কম্পিউটার দিয়ে না গিয়ে ভিপিএন সার্ভার হয়ে যাবে এবং এই ট্র্যান্সমিশন সম্পূর্ণ এনক্রিপটেড হয়ে থাকে, তাই আপনার আইএসপি কখনোই বলতে পারবে না, আপনি ইন্টারনেটে কি বা কোন ওয়েবসাইট ভিজিট করছেন। যেহেতু আপনি ভিপিএন সার্ভারে কানেক্ট হয়ে ইন্টারনেট ব্যবহার করছেন, আর সেই সার্ভার অন্য কোন দেশে অবস্থিত, তাই আপনার পাবলিক আইপি অ্যাড্রেসও ভার্চুয়াল ভাবে পরিবর্তন হয়ে অন্য দেশের হয়ে যাবে। অনেক ভিপিএন সার্ভিস প্রভাইডার রয়েছে, যারা ফ্রী এবং পেইড সার্ভিস প্রদান করে থাকে। যদি টেস্ট করতে চান সেক্ষেত্রে ফ্রী ভিপিএন ব্যবহার করে দেখতে পারেন, কিন্তু পার্মানেন্ট ব্যবহার করার জন্য, অবশ্যই আমি পেইড সার্ভিস গ্রহন করতে

বলবো। এমন কোন ভিপিএন প্রভাইডার থেকে সার্ভিস নেওয়া প্রয়োজনীয় যারা লগ সেভ করে রাখে না। তবে ভিপিএনও ট্রেস করা সম্ভব। ভিপিএন ব্যবহার করে সম্পূর্ণ কম্পিউটার বা সম্পূর্ণ নেটওয়ার্ক ট্র্যাফিক হাইড করা সম্ভব। যদি আপনার শুধু নির্দিষ্ট দুই একটা ওয়েবসাইট আনব্লক করার প্রয়োজন হয়, সেক্ষেত্রে ওয়েব প্রক্সি ব্যবহার করতে পারেন। গুগলে গিয়ে জাস্ট “web proxy” লিখে সার্চ দিলেই অনেক ওয়েবসাইট পেয়ে যাবেন, যাদের মধ্য থেকে অন্যান্য সাইট ভিজিট করতে পারবেন, এতে আপনার আইপি অ্যাড্রেস ভিসিট করা ওয়েব সার্ভার এর কাছে পৌঁছাবে না। ম্যানুয়াল প্রক্সি ব্যবহার করেও আইপি হাইড করা যায়, কিন্তু এক্ষেত্রে আসল আইপি লিক হয়ে যায়, তাই বেস্ট পদ্ধতি হচ্ছে ভিপিএন ব্যবহার করা। অনেক আইএসপি ডাইন্যামিক আইপি অ্যাড্রেস ব্যবহার করে, মানে আপনি ইন্টারনেট ডিস কানেক্ট করে কানেক্ট করলেই আপনার আইপি পরিবর্তন হয়ে যাবে। বিশেষ করে মোবাইল অপারেটর’রা ডাইন্যামিক আইপি ব্যবহার করে থাকে।

(ওয়েবসাইট আইপি খুঁজে বের করা)

দুনিয়ার যেকোনো ওয়েবসাইটের কমপক্ষে ১টি আইপি অ্যাড্রেস থাকতেই হবে। ওয়েবসাইটের আইপি অ্যাড্রেস জানার অনেক সুবিধা রয়েছে, যদি ওয়েবসাইট’টি ব্লক থাকে বাইপাস করে নিতে পারবেন, আপনি যদি কোন নেটওয়ার্কের অ্যাডমিন হোন যেকোনো ওয়েবসাইট’কে ব্লক করতে পারবেন, ওয়েবসাইটির সার্ভার কোথায় অবস্থিত সে সম্পর্কে ধারণা নিতে পারবেন, এবং আরো অনেক কিছু।আপনার ওয়েব ব্রাউজারে যখন ডোমেইন নেম প্রবেশ করান ,অবশ্যই আপনার ব্রাউজার প্রথমে আইপি অ্যাড্রেসই খুঁজে বের করে, তারপরে ওয়েবসাইট’টি লোড হয়, কিন্তু এই প্রসেস পেছনের দিকে হয়, ফলে আইপি তথ্য ব্রাউজারে প্রদর্শিত করে না। আবার বড় বড় ওয়েবসাইট গুলো একসাথে অনেক আইপি অ্যাড্রেস ব্যবহার করে, পৃথিবীর আলাদা প্রান্ত থেকে একই ডোমেইন ব্যবহার করে আলাদা আইপি থেকে সাইট লোড হয়। আপনি পিং কম্যান্ড ব্যবহার করে অনেক সহজেই যেকোনো সাইটের আইপি অ্যাড্রেস খুঁজে পেতে পারেন। উইন্ডোজ কম্পিউটার থেকে সিএমডি ব্যবহার করে জাস্ট কম্যান্ড প্রবেশ করান, “ping sobuzbanglatv.com” (যেকোনো সাইটের নাম প্রবেশ করাতে পারেন) তারপরে এন্টার হিট করলেই “Pinging sibuzbanglatv.com [104.18.41.194] with 32 bytes of data” ডোমেইন থেকে আইপি অ্যাড্রেস বের হয়ে যাবে। যদি মোবাইল ডিভাইজ থেকে এই কাজ

করতে চান গুগল প্লে এবং অ্যাপ স্টোরে অনেক অ্যাপ রয়েছে যেগুলো ব্যবহার করে ওয়েবসাইট পিং করতে পারবেন এবং আইপি খুঁজে পেতে পারবেন। যদি কোন ঝামেলায় করতে না চান, জাস্ট গুগলে যান আর ডোমেইন নেম প্রবেশ করান, আইপি অ্যাড্রেস পেয়ে যাবেন।

(ইমেইল থেকে সেন্ডারের আইপি অ্যাড্রেস বের করা)

হ্যাকিং এর ক্ষেত্রে এরকমটা আপনার বহুবার প্রয়োজনীয় হতে পারে, সামনের ব্যাক্তির আইপি অ্যাড্রেস প্রয়োজনীয় হতে পারে। সেক্ষেত্রে যে কারো আইপি কিভাবে খুঁজে পাবেন? সৌভাগ্যবসত ইমেইলকে এমনভাবে ডিজাইন করা হয়েছে, ইমেইল যে কম্পিউটার থেকে সেন্ড করা হয়েছে, সেই কম্পিউটারের আইপি অ্যাড্রেস মেইল ম্যাসেজের সাথে জুড়ে যায়। মেইল ডেলেভারি'র সময় তার হেডার থেকে সেন্ডারের আইপি অ্যাড্রেস খুঁজে পাওয়া যায়। আজকের দিনে মেইল হেডারে আর কেউ ধ্যানই দেয় না, কেনোনা মডার্ন মেইল ক্লায়েন্ট গুলো মেইল হেডারকে হাইড করে রাখে। আপনি যদি জিমেইল ব্যবহার করে থাকেন, ঐ মেইলটি খুলুন যেটার হেডার চেক করতে চান। এবার উপরের দিকে ডানপাশে আইকনের পাশে ডাউন আর্যো কী'তে ক্লিক করুণ, একটি মেন্যু খুলে যাবে, মেন্যু থেকে "Show original" এ ক্লিক করুণ, ব্যাস নিচের মতো মেইল হেডার খুলে যাবে। কিন্তু গুগল জিমেইল হেডার থেকে সেন্ডারের আইপি অ্যাড্রেস বাদ দিয়ে দেয়, শুধু গুগল সার্ভার আইপি যুক্ত করা থাকে, এই অবস্থায় আইপি অ্যাড্রেস খুঁজে পাওয়া অসম্ভব। মাইক্রোসফট হটমেইল সার্ভিসে এক্সটেন্ডেড হেডার সেন্ড করে যেটাকে "X-Originating-IP" বলা হয়, এতে সেন্ডারের আসল আইপি পাওয়া যায়, ইয়াহু মেইল হেডারে Received: entry. থেকে আইপি অ্যাড্রেস খুঁজে পাওয়া যায়।

(আইপি লোকেশন)

আইপি অ্যাড্রেস থেকে একেবারে সঠিক জিওগ্রাফিক লোকেশন খুঁজে পাওয়া সম্ভব নয়। বিশেষ করে আপনি যদি মোবাইল ইন্টারনেট ব্যবহার করে থাকেন, আপনাকে ডাইন্যামিক আইপি অ্যাড্রেস দেওয়া হয়, যেটা প্রত্যেকবার ডিস-কানেক্ট হওয়ার সময় পরিবর্তন হয়ে যায়। তবে আইপি অ্যাড্রেস থেকে আপনার আইএসপির জিও লোকেশন পাওয়া যেতে পারে, তবে সেটা ১০০% নির্ভুল হয়

না। বাইরের দেশে আইপি অ্যাড্রেস অনেক মানুষের নামে রেজিস্টার থাকে, তাদের মোবাইল নাম্বার বা আরো গুরুত্বপূর্ণ ইনফরমেশন ডাটাবেজে থাকে, সেগুলোকে এই সাইট থেকে চেক করতে পারবেন। তবে একদম ব্যবহারকারীর সঠিক লোকেশন পাওয়া না গেলেও ব্যবহারকারী কোন দেশ থেকে বা কোন আইএসপি'র সাথে কানেক্টেড এই তথ্য গুলো পাওয়া যেতে পারে। তবে সিটি সম্পর্কে সঠিক ধারণা পাওয়া যায় না, আইপি জিও লোকেশন টুল গুলো শুধু আইএসপির সার্ভার লোকেশন ডিটেক্ট করতে পারে, এখন আইএসপি যদি অনেক বড় হয়, সেক্ষেত্রে ব্যবহারকারী কোন শহরে রয়েছে নির্ণয় করা মুশকিল। আপনি যদি গ্রামীণফোন মোবাইল ইন্টারনেট ব্যবহার করেন রাজশাহী থেকে, তো আপনার আইপি লোকেশন ঢাকা শো করবে। iplocatuon.net সাইটটি থেকে যেকোনো আইপি অ্যাড্রেস আইএসপি বা কোন কোম্পানির নামে রেজিস্ট্রেশন করা রয়েছে তার তথ্য গুলো পেয়ে যেতে পারেন!

১২৭.০.০.১ লোকাল হোস্ট

১২৭.০.০.১ একটি আইপি ভার্সন ৪ আইপি অ্যাড্রেস, যেটাকে লোকাল হোস্ট বলা হয়। প্রত্যেকটি কম্পিউটার এই অ্যাড্রেসকে নিজের হোম বলে দাবী করে, কিন্তু এই অ্যাড্রেস আলাদা কম্পিউটারের সাথে যোগাযোগ করার জন্য ব্যবহার করা যায় না। আপনার কম্পিউটারে রাউটার থেকে হয়তো ১৯২.১৬৮.১.১৫ এরকম আইপি অ্যাড্রেস পেয়ে থাকে, সেটা ব্যবহার করে কম্পিউটার লোকাল এরিয়া নেটওয়ার্কের সবকিছুর সাথে যোগাযোগ ঠিক রাখে, কিন্তু তারপরেও কম্পিউটার ১২৭.০.০.১ কে "This Computer" হিসেবে দাবী করে। এটাকে লুপব্যাক আইপি অ্যাড্রেসও বলতে পারেন। ধরুন আপনার নিজের কম্পিউটারকে ওয়েব সার্ভার বানিয়েছেন, এক্ষেত্রে লোকাল হোস্ট আইপি অ্যাড্রেস ব্যবহার করে ব্রাউজারে পেজ গুলোকে লোড করতে পারবেন। যখন ১২৭.০.০.১ আইপি অ্যাড্রেস ব্রাউজারে প্রবেশ করাবেন, ব্রাউজার নেটওয়ার্কের মধ্যে পেজ না খুঁজে আপনার কম্পিউটারেই পেজটি খুঁজবে। কেনোনা এটি হোম অ্যাড্রেস! আপনার কম্পিউটার থেকে লোকাল হোস্ট রিকোয়েস্ট করা হলে সেটা কম্পিউটারেই সীমাবদ্ধ থাকবে, লোকাল এরিয়া নেটওয়ার্ক বা ইন্টারনেটে সেই রিকোয়েস্ট কখনোই যাবে না।

(ডিএইচসিপি) (DHCP)

ডিএইচসিপি এর পূর্ণাঙ্গ নাম ডাইন্যামিক হোস্ট কনফিগারেশন প্রোটোকল। এটি এমন একটি প্রোটোকল যার মাধ্যমে নেটওয়ার্কে দ্রুত, স্বয়ংক্রিয় এবং সেন্ট্রাল আইপি অ্যাড্রেস ডিস্ট্রিবিউশন ম্যানেজ করা হয়। সত্যি বলতে আপনার রাউটার একটি ডিএইচসিপি সার্ভার হিসেবে কাজ করে, যেটা সকল ডিভাইজে স্বয়ংক্রিয়ভাবে ইউনিক আইপি অ্যাড্রেস বন্টন করে থাকে এবং এই প্রক্রিয়া সম্পূর্ণই স্বয়ংক্রিয় হয়ে থাকে। যখন একটি ডিভাইজ অন হয় এবং রাউটারের কাছে কানেক্ট হওয়ার জন্য রিকোয়েস্ট প্রদান করে সেটাকে DHCPDISCOVER রিকোয়েস্ট বলা হয়। এক্ষেত্রে ডিভাইজ কানেক্ট হওয়ার জন্য রাউটারের কাছ থেকে নতুন আইপি অ্যাড্রেস চেয়ে রিকোয়েস্ট করে। ডিসকভার রিকোয়েস্ট প্যাকেট ডিএইচসিপি সার্ভারের কাছে পৌছার পরে, সার্ভার একটি আইপি অ্যাড্রেস তৈরি করে দেয় যেটা ডিভাইজটি ব্যবহার করে কানেক্ট হতে পারে। সার্ভার থেকে আইপি পাওয়ার পরে ডিভাইজটি আবার DHCPREQUEST প্যাকেট সেন্ড করে নেটওয়ার্কে কাজ করার জন্য। যদি সার্ভার দেখে আইপি অ্যাড্রেস ঠিক আছে আর কানেকশন দেওয়া যাবে, একটি হ্যাঁ মূলক রেসপন্স করে। এই রিকোয়েস্ট গুলো অনেক দ্রুত প্রসেস হয়ে যায়, তাই ইউজার এগুলোর সম্পর্কে কিছু বোঝারই প্রয়োজন পরে না। ডিএইচসিপি ডাইন্যামিক আইপি স্টাইল ব্যবহার করে, তাই একই লোকাল নেটওয়ার্কে কখনোই সেম আইপির দুইটি ডিভাইজ তৈরি হবে না, আর এটা সম্পূর্ণই স্বয়ংক্রিয়।

(ম্যাক অ্যাড্রেস খোঁজা)

টিসিপি/আইপি কম্পিউটার নেটওয়ার্কে আইপি অ্যাড্রেস এবং ম্যাক অ্যাড্রেস একসাথে ব্যবহৃত হয়। যেখানে আইপি অ্যাড্রেস গুলো ভার্চুয়াল অ্যাড্রেস যেটা নেটওয়ার্কে বারবার পরিবর্তন হতে পারে, কিন্তু ম্যাক অ্যাড্রেস পার্মানেন্ট অ্যাড্রেস হয়ে থাকে, যেটা কখনোই পরিবর্তন হয় না। ম্যাক অ্যাড্রেস সাধারণত নেটওয়ার্ক ইন্টারফেস অনুসারে আলাদা আলাদা হয়ে থাকে। যেমন আপনার ল্যাপটপে ব্লুটুথ, ওয়াইফাই, এবং ইথারনেট রয়েছে, সেই ক্ষেত্রে আপনার ল্যাপটপে ০৩ টি ম্যাক অ্যাড্রেস থাকবে। যদি একসাথে দুইটি ওয়াইফাই অ্যাডাপ্টার ব্যবহার করেন, তাহলে দুইটি ওয়াইফাই এর জন্য আলাদা আলাদা ম্যাক অ্যাড্রেস থাকবে।

অনেক গুরুত্বপূর্ণ কারণ রয়েছে যার জন্য ডিভাইজ ম্যাক অ্যাড্রেস আপনার জানা প্রয়োজনীয় হতে পারে। ধরুন আপনি নেটওয়ার্কে যদি ম্যাক অ্যাড্রেস ফিল্টার করে রাখেন, তাহলে শুধু মাত্র নির্দিষ্ট ডিভাইজই রাউটারের সাথে কানেক্টেড হতে পারবে, পাসওয়ার্ড জেনেও লাভ নাই, অন্য ডিভাইজকে রাউটার অ্যালাউ করবে না। তাছাড়া ম্যাক অ্যাড্রেস থেকে ডিভাইজ প্রস্তুতকারী কোম্পানি সম্পর্কে জানতে পারা যায়।

আপাততো কোন ডিভাইজ যদি ফিজিক্যালভাবে রিচ না করতে পারেন, এর ম্যাক অ্যাড্রেস পাওয়া সম্ভব হবে না। আইপি অ্যাড্রেস আর ম্যাক অ্যাড্রেস আলাদা দুইটি জিনিষ। তবে আপনার কম্পিউটার যদি একই লোকাল নেটওয়ার্কে কানেক্টেড থাকে, সেক্ষেত্রে লোকাল নেটওয়ার্ক ডিভাইজের ম্যাক অ্যাড্রেস পেয়ে যেতে পারবেন। আপনাকে কম্যান্ড প্রমট ওপেন করতে হবে এবং কম্যান্ড দিতে হবে “ping 192.168.45.15” এখানে যে ডিভাইজের ম্যাক দেখতে চান তার আইপি দিতে হবে। ডিভাইজটি পিং রিসিভ করলে ঠিক এইরকম নিচের মতো রেসপন্স দেখতে পাবেন। Pinging 192.168.86.45 with 32 bytes of data: Reply from 192.168.45.15: bytes=32 time=290ms TTL=128 Reply from 192.168.45.15: bytes=32 time=3ms TTL=128 Reply from 192.168.45.15: bytes=32 time=176ms TTL=128 Reply from 192.168.45.15: bytes=32 time=3ms TTL=128 এবার সেম কম্যান্ড সেশনে “arp -a” কম্যান্ডটি প্রবেশ করান, এতে পিং করা ডিভাইজটির ম্যাক অ্যাড্রেস দেখতে পাবেন।ঠিক নিচের মতো রেসপন্স রিসিভ হবে Interface: 192.168.45.15 --- 0x3 Internet Address Physical Address Type 192.168.45.1 70-3a-cb-14-11-7a dynamic 192.168.45.15 98-90-96-B9-9D-61 dynamic 192.168.45.255 ff-ff-ff-ff-ff-ff static 224.0.0.22 01-00-5e-00-00-16 static 224.0.0.251 01-00-5e-00-00-fb static তবে এই পদ্ধতি কাজে লাগিয়ে ইন্টারনেটের মাধ্যমে ডিভাইজ ম্যাক দেখা সম্ভব হবে না, শুধু লোকাল নেটওয়ার্কে এটি কাজে দেবে। এই ম্যাক অ্যাড্রেস আসলে ক্যাশ থেকে শো করে এবং অ্যাড্রেস রেজুলেসন প্রোটোকল ব্যবহার করে আপনি সেটাকে দেখতে পান। সামনের পর্বে ম্যাক অ্যাড্রেস নিয়ে আরো বিস্তারিত আলোচনা করবো, যেভাবে এই পর্বে আইপি অ্যাড্রেস কভার করছি!

(আইপি অ্যাড্রেস ফরওয়ার্ড এবং রিভার্স লুকাপ)

আইপি লুকাপ বলতে সেই প্রসেসকে বুঝানো হয়, যখন ইন্টারনেট ডোমেইন নেম থেকে আইপি অ্যাড্রেস ট্রান্সলেসন করা হয়। ফরওয়ার্ড আইপি লুকাপ বলতে ডোমেইন নেমকে আইপি অ্যাড্রেসে কনভার্ট এবং রিভার্স আইপি লুকাপ বলতে আইপি অ্যাড্রেস থেকে ডোমাইনে ব্যাক করার প্রসেসকে বুঝানো হয়। এই পরিভাষা গুলো আপনাকে অবশ্যই মনে রাখতে হবে, এগুলো পরবর্তী অ্যাডভান্স কোর্স গুলোতে কিন্তু আমি বার বার বর্ণনা করবো না। অনেক ইন্টারনেট সার্ভিস রয়েছে যেগুলো আইপি লুকাপ এবং রিভার্স লুকাপ দুইটাই সমর্থন করে। আইপি লুকাপ করার জন্য ডিএনএস সার্ভার থেকে ডাটা নেওয়া হয়, রিভার্স লুকাপের জন্যও ডাটাবেজ থাকে। অবশ্যই প্রত্যেকটি ডোমেইন নেম সল্ভ করে সেই ওয়েব সার্ভারের সাথে কানেক্ট হতে ফরওয়ার্ড লুকাপ প্রয়োজনীয়। কিন্তু আপনি যদি জানতে চান, ঐ আইপি অ্যাড্রেসে কতো গুলো ওয়েবসাইট রয়েছে, তখন রিভার্স আইপি লুকাপ চেক করতে হবে। আপনি এই অনলাইন রিভার্স লুকাপ টুলটি ব্যবহার করে চেক করতে পারেন, ঐ সার্ভার আইপিতে আরো কতো ওয়েবসাইট হোস্ট করা রয়েছে।

এই পর্বে বেসিক জিনিষ গুলোর সাথে সাথে আপনাকে অনেক কিছু অ্যাডভান্স টার্ম গুলোও শিখিয়ে দিয়েছি। আইপি অ্যাড্রেস নিয়ে আরেকটি পর্ব আসতে পারে, যেখানে বিভিন্ন রেঞ্জের আইপি নিয়ে বিস্তারিত আলোচনা করবো, কিন্তু আপাতত দ্রুত এরকম পোস্ট পাবলিশ করছি না এই পোস্ট টাকে আর বড় করার জন্য! নেক্সট পর্বে অবশ্যই আরো টেকনিক্যাল দিকে চলে যাবো। একদমই চিনতে করবেন না, আমি যতোটকু জানি আপনাকে সবকিছুই জানিয়ে দিবো। তাই সাথেই থাকুন, আর পরবর্তী পর্বও দ্রুতই আসছে। যেকোনো প্রশ্নে এই পোস্টের নিচে কমেন্ট বক্সে অবশ্যই কমেন্ট করবেন, যদি গুন কিত্তন বা বকা-ঝকা করতে চান, তাহলে প্লিজ সবার আগে কমেন্ট করুণ!আর হ্যা আজকের ০৩ পর্বটি কেমন লাগলো জানাতে ভুলবেন না কিন্তু! আল্লাহ্ হাফেজ।

এথিক্যাল হ্যাকিং ফ্রী কোর্সঃ পর্ব - ০৪; ওয়্যারলেস নেটওয়ার্কিং (বেসিক ১)

অনেক দিন পরে শুরু করলাম, কেমন হবে জানি না। আমি জানি আমি সবুজ আপনাদেরকে তেমন ভালোমতো বুঝাতে পারিনা। তাই যদি কিছু ভুল হয়ে থাকে, তাহলে আমাকে ক্ষমাসুন্দর দৃষ্টিতে দেখবেন এবং নিজগুণে ক্ষমা করে দিবেন।(এথিক্যাল হ্যাকিং ফ্রী কোর্সঃ পর্ব -০৪,) ওয়্যারলেস নেটওয়ারকিং (বেসিক ১) এ আপনাকে স্বাগতম। গত পর্বে আমারা নেটওয়ার্কিং এর সমস্ত বিষয় গুলো জেনেছি ।

আজ আমরা আলোচনা করবো ওয়্যারলেস নেটওয়ার্কিং নিয়ে, তো বেশি কথা না বলে আসুন শুরু করা যাক ।

ওয়্যারলেস নেটওয়ার্ক কি?

ওয়্যারলেস নেটওয়ার্ক হচ্ছে রেডিও ওয়েভ দিয়ে পরিচালিত নেটওয়ার্ক। এটা মূলত বাকি ১০ টা ল্যান কানেকশনের মতই কিন্তু এখানে তারের বদলে একাধিক কম্পিউটার রেডিও ওয়েভের মাধ্যমে কানেক্টেড হয়ে থাকে। এখানে কম্পিউটার বলতে আপনি মোবাইলকে ধরতে পারেন আবার আপনার কম্পিউটার কেও ধরতে পারেন। কিন্তু একে অপরের সাথে কানেক্ট হতে চাইলে আপনাকে কোন মাধ্যমের সাহায্য নিতে হবে যেমন ধরুন ওয়াইফাই রাউটার, আপনাকে ইন্টারনেটের সাথে কানেক্ট হতে হলে রাউটারের সাথে আগে কানেক্ট হবে তারপরে আপনি ইন্টারনেটে কানেক্ট হতে পারবেন। তো বুঝতে পেরেছেন হইতো এখন আসি পরের কথায়, আপনার মাথায় প্রশ্ন আসতে পারে ওয়্যারলেস নেটওয়ার্কেও কি LAN, PAN, WAN, MAN আছে কি না? হ্যা, বন্ধুরা আছে। আপনাকে বুঝতে হবে ওয়্যারলেস শুধু মাত্র একটি নেটওয়ার্ক সিস্টেম। সাধারণ ইথারনেট কানেকশন বা ক্যবল কানেকশন যেভাবে কানেক্টেড হয়, ওয়্যারলেস নেটওয়ার্ক সেভাবে কানেক্টেড হয় না। পার্থক্য শুধুমাএ এই জায়গাতেই আর কিছু না। ওয়্যারলেস নেটওয়ার্কেরও রয়েছে LAN, PAN, WAN, MAN। আসুন আজ সংক্ষেপে জেনে নিই এই গুলো সম্পর্কেঃ ওয়্যালেস নেটওয়ার্ক কি!

(ওয়্যারলেস লোকাল এরিয়া নেটওয়ার্ক বা WLAN)

WLAN নিয়ে আলোচনা করার আগে আমি বলে রাখি,আজ শুধু এটা নিয়েই

আলোচনা করবো, বাকি সকল নেটওয়ার্ক গুলো নিয়ে আমি বিস্তারিত আলোচনা করবো না, কেননা, এই গুলো নিয়ে এর আগে আলোচনা করা আছে। WLAN বুঝার আগে আপনাকে বুঝতে হবে LAN কি?

একাধিক কম্পিউটার কোন ক্যাবলের মাধ্যমে একে অপরের সাথে সংযুক্ত হয়ে যে নেটওয়ার্ক তৈরি করে সেটাই ল্যান। কিন্তু আপনার মাথায় প্রশ্ন আসতে পারে তাহলে আমরা ব্রডব্যান্ড ব্যবহার করি সেটাও তো ল্যান লাইনের মাধ্যমে আমাদের ইন্টারনেট দিয়ে থাকে। ঠিক তখনি আপনার মাথা চন্দ্রবিন্দু হয়ে যায়, কিন্তু এখানে চিন্তা করার কিছুই নেই। আপনি শুধু ঠান্ডা মাথায় একটু ভাবুন আপনি যেই কম্পিউটার ব্যবহার করছেন তার একটা প্রাইভেট আইপি আছে কিন্তু ইন্টারনেটে আপনার আইপি চেক করলে কেন অন্য আইপি দেখায়? কেননা আপনার আইপি হিসাবে তখন কাউন্ট করা হয় আপনার আইএসপির আইপিটাকে, এর মানে আপনার প্রাইভেট আইপিটা হাইড হয়ে গেছে, কিন্তু কেন? এবার আরেকটু ভাবুন তো আপনি শুধু আপনার আইএসপি থেকে কানেকশন নিয়েছে? নাহ আরো অনেকেই নিয়েছে, সবার কিন্তু একই সম্যসা দেখা দিচ্ছে, কিন্তু কেন? কেন? কেন? এর কারণ হচ্ছে আপনি কিন্তু লোকাল এরিয়া নেটওয়ার্কের মাঝেই আছেন কিন্তু সেটা আপনার আইএসপির সাপেক্ষে। আমার কম্পিউটার আর , আপনার কম্পিউটার আর যদি অন্যান আরো অনেকগুলি কম্পিউটারের সাথে কানেক্ট থাকে, তাহলে তো সেটা লোকাল এরিয়া নেটওয়ার্ক হবে। আর যেই কম্পিউটার থেকে আপনাদের নিয়ন্ত্রণ করা হয়, সেই কম্পিউটারটা থাকে আপনার আইএসপির কাছে। ঠিক এই কারনে আপনার আইএসপির এফটিপি সার্ভার থেকে ডাওনলোড করলে অনেক ভাল স্পিড পেয়ে থাকেন, যা আপনি ইন্টারনেটের সাথে যুক্ত অন্য কম্পিউটার থেকে পাবেন না। কিন্তু আপনি যখন অন্য কম্পিউটারে ঢুকতে যাচ্ছেন অব্যশই সেটা হতে হবে আপনার লোকাল এরিয়ার বাইরে। তখন আপনি ঢুকছেন আপনার আইএসপির কম্পিউটারের সাহায্য নিয়ে আর ঠিক এই কারনেই আপনার আইপি হিসাবে আপনার প্রাইভেট আইপি দেখায় না। অনেক কথা হয়েছে ভাই আর না। এবার আসি WLAN এর কথায়। কি এটা কি আপনাকে বুঝানো লাগবে? বুঝেন নাই ব্যাপার টা? তাহলে আসেন আবার বুঝিয়ে দেই, আর যদি আগেই বুঝে থাকেন থাহলে আপনি আরেকবার বুঝে নেন, বুঝতে গেলে আমি কোন টাকা নেই না। আসলে LAN এর ব্যপারে যা যা বলেছি আপনি শুধু

সেটাকে একটু পরির্বতন করে ভাবুন। ল্যানে আপনি ব্যবহার করতেন ক্যাবল, কিন্তু WLAN আপনি ব্যবহার করছেন রেডিও ওয়েভ। এবার ভাবতে পারেন তাহলে আপনার কম্পিউটার হবে যেটা সব কিছু নিয়ন্ত্রণ করবে। আরে ভাই আছে না রাউটার, রাউটারের কাজটাই তো এটা। এটা আপনাকে রেডিও ওয়েব ছড়িয়ে কানেক্ট করে নিবে, আবার আপনার সকল কিছু নিয়ন্ত্রণ করেবে। যদি এর পরেও না বুঝেন, তাহলে সব থেকে ভাল উদাহরন ভাই আপনি কি মিনি মিলিশিয়া খেলেছেন? যদি খেলে থাকেন তাহলে আপনি কি করেন, আপনার আরো বন্ধুর সাথে একসাথে বসে আপনার মোবাইল থেকে সাবাই কে কানেক্ট করে নিয়ে খেলা শুরু করে দিলেন। কিন্তু ভেবে দেখুন আপনি কানেক্ট হয়েছেন কোথায়? কিভাবে? আপনি কানেক্ট হয়েছেন রেডিও ওয়েভের মাধ্যমে আর আর আপনি কানেক্ট হয়েছেন আপনার বন্ধুদের সাথে। এর অর্থ আপনি WLAN কানেক্ট করে নিয়েছেন। শুধু কি তাই আপনার ফোনটা একই সাথে রাউটারের কাজ টাও করে ফেলছে। একটা কথা আমি জানি আপনার মাথায় অনেক চিন্তা ও অনেক প্রশ্ন আসবে LAN ও WLAN নিয়ে আরো আলোচনা করা হবে। কিন্তু বেসিক পর্বে এত কিছু আলোচনা করলে আপনি কিছুই বুঝতে পারবেন না। তাই এবার যাই পরের কাহিনিতে।

(ওয়্যারলেস মেট্রোপলিটন এরিয়া নেটওয়ার্ক (WMAN)

আপনারা হয়তো বুঝতে পেরেছেন WMAN বলতে আমি কি বুঝাতে চেয়েছি? সহজ কথায় WMAN হচ্ছে MAN এর ওয়ারলেস ভার্সন, MAN নেটওয়ার্কে যেখানে তার বা ক্যাবল ব্যবহার করা হত WMAN এ ওয়্যারলেস মানে রেডিও ওয়েভ ব্যবহার করা হয়।এইখানেও আপনাকে যদি WMAN নেটওয়ার্ক কে বুঝতে হয় আপনাকে তার আগে MAN নেটওয়্যার্কে বুঝতে হবে। MAN হচ্ছে মেট্রোপলিটন এরিয়া নেটওয়ার্ক যদি এখানে মেট্রপলিটন এরিয়া নেটওয়ার্ক বলতে বুঝানো হয়েছে অনেক গুলো ল্যান লাইনকে এক সাথে সংযোগ করে নতুন ইন্টারফেস দেয়া। যেমন আমি ঢাকা শহরে থাকি এবার আমার শহরের বিভিন্ন স্থানে ল্যান সংযোগ লাগানো হয়েছে, এখন সব গুলো লাইন আমাদের ঢাকা শহর কভার করে ফেলেছে। এখন এটাই হচ্ছে মেট্রোপলিটন এরিয়া নেটওয়ার্ক। তবে এর সব থেকে বড় উদাহরণ হিসাবে আপনি ধরতে পারেন আপনার ব্রডব্যান্ড কম্পানিকে। এবার আপনি যদি আপনার শহরকে কভার

করতে অনেক গুলো ল্যান লাইন কে ওয়্যারলেসের সাথে কানেক্ট করে অনেক যায়গাই স্থাপন করেন এবং সেটার মাধ্যমে আপনি পুরো শহর কভার করেন তবে সেটা হচ্ছে ওয়্যারলেস মেট্রোপলিটন এরিয়া নেটওয়ার্ক। আশা করি বুঝতে পেরেছেন।

(পার্সোনাল এরিয়া নেটওয়ার্ক (PAN)

নাম শুনেই হয়তো বুঝতে পেরেছেন PAN আসলে কেমন হতে পরে! হা, ঠিকি ধরেছেন PAN মূলত পার্সোনাল কাজের জন্য ব্যবহার করা নেটওয়ার্ক। এবার আপনি বলতে পারেন ভাই আপনি এইখানে PAN বলেছেন কিন্ত WPAN বলেন নি কেন? আসলে ভাই PAN বলতে গেলে মূলত ওয়্যারলেসের ব্যাপারটাই আসে, তাছাড়া এই ব্যাপারটা নিয়ে হয়তো অনেকেই জানেন না তাই আলাদা করে কিছু লিখি নাই। PAN এর বড় উদাহরন হিসাবে আপনি ধরে নিতে পারেন আপনার মোবাইলের হট স্পটকে। যেখানে আপনি আপনার মোবাইল দিয়ে ওয়েভ ছড়াচ্ছেন এবং আপনার নেটওয়ার্কের আওতাই আরো অনেকে আছে। তবে একটা বিষয় জেনে রাখুন PAN নেটওয়ার্ক কিন্তু LAN নেটওয়ার্কের ক্ষুর্দ সংস্করন। কেননা PAN নেটওয়ার্ক বানাতে গেলে নিশ্চিত ভাবে আপনাকে LAN বা WLAN বানানো লাগবেন। আশাকরি বুঝতে পেরেছেন।

(ভার্চুয়াল প্রাইভেট সার্ভার) (VPN)

নাম শুনেই বোঝা যাচ্ছে এই নামটা অনেক আগে থেকেই শুনে এসেছি আমরা, অনেকেই হইতো অনেক কাজেই এটাকে সফটওয়্যার হিসাবে ব্যবহার করে থাকি। কিন্তু এটা কোন সফটওয়্যার না, এটা মূলত হচ্ছে একটা নেটওয়ার্ক। আসুন তাহলে একটু বুঝে নিই, VPN মূলত সার্ভার কেন্দ্রিক নেটওয়ার্ক (সার্ভার কথাটি বোঝানোর জন্য বলা হয়েছে)। এখন সার্ভার টা কি? সার্ভার বলতে এখানে বোঝানো হয়েছে অন্য কোন স্থানে রাখা কম্পিউটার। এর আসলে কোন শরীরি অবস্থান নেই। কিন্তু পৃথিবীর অনেক স্থান থেকে অনেকেই এই সার্ভারের সাথে যুক্ত হতে পারে। এটাকে অনেক ক্ষেত্রে EPN বা Enterprise Private Network বলা হয়ে থাকে। কেননা অনেক ক্ষেত্রে অনেকে এটাকে ক্রয় করে ব্যবহার করে থাকেন।

(হোম রাউটার কমপ্লিট সেটআপ)

অনেকে এটা একটি অহেতুক লেখা হিসাবে ধরে নিতে পারেন কিন্তু বিশ্বাস করুন আপনি এটাকে অহেতুক ভাবলেও এটা অহেতুক না। আপনি যদি নিজের সিকিউরিটি নিজে দিতে না পারেন, তাহলে আপনি তো এথিক্যাল হ্যাকার হতে পারবেন না। তাছাড়া শুধু মাএ রাউটার হ্যাক করেই, আপনি অনেক কিছু হ্যাক করার সামর্থ রাখেন। বিস্তারিত ভাবে আপনাদের আস্তে আস্তে শেখানো হবে। তাহলে চলুন জেনে নিই কিভাবে হোম রাউটার কমপ্লিট ভাবে সেট আপ করবেন।

(বেসিক কনফিগারেশন ও কানেকশন)

বেসিক কনফিগারশন বলতে এই ধাপে আপনি জানবেন কিভাবে রাউটার টা কানেকশন করানো হয় ও সাধারণ কনফিগারেশন। তাহলে চলুন জেনে নিই।

১। প্রথমে আপনার রাউটার টা ল্যান লাইনের সাথে সংযুক্ত করুন।

২। এবার আপনার রাউটারের পেছনে দেখেন কিছু পোর্ট বা হাব আছে সেই গুলোর সাথে আপনার ইথারনেট কেবল টা যুক্ত করুন এবং সেটা আপনার কম্পিউটারের ল্যান পোর্টের সাথে যংযুক্ত করুন। যদি কেও ইথারনেট ক্যাবল ব্যবহার করতে না চান, সেই ক্ষেত্রে আপনি আপনার রাউটারের বক্সে বা রাউটের পেছনে দেখুন একটা পাসওয়ার্ড দেয়া আছে। এবার আপনি আপনার ওয়াই-ফাইটা সেই পাসওয়ার্ড দিয়ে কানেক্ট করুন। যদিও কিছু কিছু রাউটারের অটমেটিক ভাবে কানেকশন নিয়ে নেয়।

৩। এবার আপনার কম্পিউটারের বা মোবাইল ডিভাইসের যেকোন ব্রাউজারে গিয়ে 192.168.1.1 অথবা 192.168.0.1 এই আইপি ঢুকুন। এইটা হচ্ছে আপনার লোকাল আইপি প্রায় সকল রাউটারে এইটাই ডিফল্ট হিসাবে থাকে।

৪। আপনার সামনে একটা পেজ আসবে, মানে লগইন পেজ ডিফল্ট ইউজার নেম পাসওয়ার্ড দিয়ে লগইন করুন। যেহেতু আমি টিপি-লিঙ্ক রাউটার ব্যবহার

করি সেহেতু আমার ডিফল্ট ইউজার নেম ও পাসওয়ার্ড হচ্ছে admin:admin । কিন্তু সকল কোম্পানির রাউটারের ডিফল্ট ইউজার নেম ও পাসওয়ার্ড একই না। সেটা জানার জন্য আপনি আপনার রাউটারের ইন্সট্রাকশন বইটা একটু পড়ে নিন, সেখানে দেওয়া আছে। যদি ৮০% ওয়াই-ফাই ব্যবহার কারী টিপি-লিংক ব্যবহার করে।

৫। আপনি এবার একটা পেজ পাবেন, যদিও সব রাউটারে একই ইন্টারফেস না। কিন্তু নিয়ম প্রায় সকল রাউটারের একই। এবার আপনি Quick Setup পেজে ক্লিক করুন। তাহলে আপনি নতুন পেজে ঢুকে যাবেন।

৬। এবার আপনি ওপরের মত একটা পেজ পাবেন, যদি প্রথম স্টেপে না পান, তবে Next করবার কোন অপশন থাকতে পারে। যাই হোক আপনি এই পেজে ঢুকার পরে আপনি Auto-Detection ক্লিক করে Next এ ক্লিক করুন। কেননা আপনি যদি না জেনে থাকেন আপনারটা কি কানেকশন, তবে এটা আপনাকে অটোমেটিক সেট আপ পেজে নিয়ে যাবে। যদি আপনার WAN কানেকশনটি PPPoE কানেকশন হয় তবে আপনি একটা পেজ পাবেন। এবার আপনার ইউজার নেম ও পাসওয়ার্ড দিয়ে আপনি লগইন করে ফেলুন। যদি আপনি এটা না জানেন, তবে আপনার আইএসপির সাথে যোগাযোগ করে ইউজার নেম ও পাসওয়ার্ড নিয়ে নিন। যদি আপনার Static IP বা Real Ip হয় তবে আপনার সামনে একটি পেজ আসবে, সেইখানে আপনার আইপি এড্রেস ও গেটওয়ে মাস্ক সব কিছু বসিয়ে সেভ করিয়ে দিন। এই গুলো আপনি আপনার আইএসপি কোম্পানির কাছে থেকে নিয়ে নিবেন।

(ওয়াই-ফাই সেট আপ)

যেহেতু আপনি ওয়াই-ফাই চালাবেন তাই রাউটার কিনেছেন এখন তো আপনাকে ওয়াই-ফাই সেট আপ করতে হবে। আসুন দেখে নিই কিভাবে ওয়াই-ফাই সেট আপ করবেন।

১। প্রথমে আপনি Wireless বা Wireless Settings এ যাবেন, সেই খানে থেকে আপনি আপনার SSID বা আপনার ওয়াই-ফাই এর নাম দিবেন ও আপনার

password Create করুন।

২। ওয়াই-ফাই এর পাসওয়ার্ড ইনক্রিপশন হিসাবে অব্যশয় WPA-PSK/WPA2-PSK সিলেক্ট করে দিন। কেননা এটাই হচ্ছে সব থেকে আপডেট ওয়াই-ফাই ইনক্রিপশন ফরমেট।

কিভাবে আপনার ওয়াই-ফাইকে আরো সিকিউর করবেন।

নিরাপত্তা বা সিকিউরিটি হচ্ছে সব গুরুত্বপূর্ণ বিষয়, কেননা আপনি যদি আপনার ওয়াই-ফাইকে যথেষ্ঠ সিকিউরিটি না দিতে পারেন আপনার ওয়াই-ফাই যেকোন সময় হ্যাক হবার সম্ভাবনা থেকে যায়। তাহলে আপনি আর কি করতে পারেন আপনার ওয়াই-ফাই কে নিরাপদ রাখতে? টেনশন নিবেন না, সবুজ বাংলা ইউটিউব হেল্পলাইন আছে আপনার পাশে।

১। আমাদের সব থেকে বড় যে ভুলটা করে থাকি, সেটা হচ্ছে আমাদের রাউটারের ডিফল্ট ইউজার নেম ও পাসওয়ার্ড আমরা পরিবর্তন করি না। কিন্তু এটা হচ্ছে সব থেকে বড় ভুল। কেননা ডিফল্ট ইউজার নেম ও পাসওয়ার্ড কোন কিছুতেই ব্যবহার করা ঠিক না। তাই খুব দ্রুত আপনি এটা পরিবর্তন করে নিন। কিভাবে করবেন? প্রথমে আপনি রাউটারের কন্ট্রোল প্যানেলে যান> System Tools > Password এবং আপনি আপনার পাসওয়ার্ড ও ইউজার নেমটি পরিবর্তন করুন।

২। আমরা আরেক টা ভুল করি সেটা হচ্ছে, আমাদের ওয়াই-ফাই এর পাসওয়ার্ড আমরা ছোট ও সাধারণ পাসওয়ার্ড দেয়। কিন্তু এটা মারাত্বক একটা ভুল, আপনার পাসওয়ার্ড আপনি কখনো ১৫ ওয়ার্ডের নিচে রাখবেন না। সেটার মাঝে অব্যশয় স্পেশাল কিছু ওয়ার্ড রাখবেন যেমনঃ .<.>?/'";:[{]})(-_+=@!$#%& এই গুলো, তাছাড়া আপনি upercase, lower case এই গুলো ব্যবহার করবেন।

৩। অনেক সময় আমরা আমাদের রাউটারের Fairwall আনেবল করি না। কিন্তু এটা খুব জরুরি কেননা Fairwall হচ্ছে সব কিছু থেকে বাচানোর সুরক্ষা দেওয়াল, আর আপনি যদি সেটা আনেবল না করে থাকেন, তাহলে বুঝতেই

পারছেন আপনি কতটা বোকার মত কাজ করেছেন। তাই খুব দ্রুত আপনার রাউটারের fairwall টা আনেবল করে নিন।

৪। WPS ডিসেবল করে নিন। যদি আপনি আপনার রাউটার কে অফিসে ব্যবহার না করেন বা WPS এর যদি দরকার না থাকে তবে আপনি ভুলেও WPS Enable রাখবেন না।

৫। পাসওয়ার্ড ইনক্রিপশন হিসাবে আপনি WEP ভুলেও ব্যবহার করবেন না। WPA / WPA2 এই গুলোই এখন ভার্নেবল হয়ে গেছে, তাই নতুন ইনক্রিপশন আপডেট হিসাবে এসেছে WPA-PSK/WPA2-PSK। আপনি অব্যশয় এই এনপক্রিপশন ফরমেটটা ব্যবহার করবেন।

কিভাবে আপনি শক্তিশালী পাসওয়ার্ড সিলেক্ট করবেন?

অনেক সময় আমরা আমাদের পাসওয়ার্ড দেওয়ার সময় ছোট পাসওয়ার্ড দিয়ে থাকি আর কারণ হিসাবে বলে থাকি আমার বড় পাসওয়ার্ড মনে থাকে না, কিন্তু এটা কোন যুক্তি সংগত কথা না।যদি না জেনে থাকেন কিভাবে শক্তিশালি পাসওয়ার্ড বানাবেন? কিছু স্টেপ আপনি ফলো করুন আশা করছি আপনি আপনার ওয়াই-ফাই টা অনেক সুরক্ষিত রাখতে পারবেন।

১। ১৫ টা ওয়ার্ডের নিচে কখনো পাসওয়ার্ড দিবেন না।

২। আপনার পাসওয়ার্ডে আপনি স্পেশাল ওয়ার্ড যুক্ত করুন কিছু, যেমনঃ !@#$%^&*()_+}{][ইত্যাদি

৩। নিজে নিজে পাসওয়ার্ডের একটা প্যাটান বানান, এবার সেই প্যাটান হিসাবে পাসওয়ার্ড দিন যেমনঃ আমার নাম Pappu, আমার GF এর নাম Samira (শুধু শেখার জন্য দেওয়া হয়েছে এই নাম গুলো কাকতালিও) ।এখন আমি আমার পাসওয়ার্ড হিসাবে যদি PappuSamira এইটা দিই তাহলে সেটা হবে বোকামি। কখনোই এমন পাসওয়ার্ড দিবেন না। আপনি আগে ভেবে নেই আপনার প্রিয় সংখ্যা কি? যেমন আমার 2 তাই আমি দিব P এর কাছে 2 তাহলে আমার পাসওয়ার্ড টা হচ্ছে 2a22uSamira কিন্তু আপনি যদি চান এটা দিবেন তাহলে

আমি আপনাকে এটা রিকমান্ড করবো না কেননা আমি আরো সিকিউরিটি চাই। তাই আমি এবার এই পাসওয়ার্ডের সামনে, পেছনে, মাঝে সব জায়গা তেই কিছু স্পেশাল ওয়ার্ড দিব। কেননা আগেই বলা ছিল ১৫ ওয়ার্ডের নিচে পাসওয়ার্ড দেওয়া যাবে না। তাই 2a22uSamira এর সাথে কিছু যোগ করবো, Pappu > 2a22u এর আগে একটা ! ও একটা @ দেন। কেননা !@ এই ২ টা ওয়ার্ড ব্যবহার হয় Shift মেরে ১৩২ চাপলে তাহলে তো আপনার মনে রাখা সুবিধা। তাহলে পাসওয়ার্ড হচ্ছে !@2a22uSamira , এবার তাহলে আমি মনে রাখার জন্য Pappu ও Samira এই ২ টা ওয়ার্ডের মাঝে + দিব। তাহলে পাসওয়ার্ড হচ্ছে !@2a22u+Samira কিন্তু আমাদের আরো একটা অক্ষর দিতে হবে যেহেতু আমাদের টার্গেট ১৫ তা আক্ষর তাই আমরা আমাদের পাসওয়ার্ডের শেষে একটা ? বসায় দিব তাহলে আমার পাসওয়ার্ড হচ্ছে !@2a22u+Samira? এবার আপনি বলেন আপনার পাসওয়ার্ড মনে রাখা কি খুব বেশি ঝামেলা হয়ে গেল? আমি বলছি না যে আপনি এই প্যাটানে পাসওয়ার্ড বানান আমি শুধু আপনাদের বোঝানোর জন্য এমন টা দিয়েছি। আপনার প্যাটান আপনি নিজে তৈরি করুন।

আজ অনেক দিন পরে লিখতে বসেছিলাম, জানিনা কেমন হয়েছে। আশা করছি আপনাদের ভাল লাগবে, যদি ভাল লাগে সেটাও কমেন্ট করে জানাবেন, যদি ভাল না লাগে সেটাও কমেন্ট করে জানাবেন। কেননা আপনার কমেন্ট আমাকে উজ্জিবিত করে, আপনাদের কমেন্ট আমাকে নতুন করে ভাবতে শেখায়। আল্লাহ হাফেজ! দেখা হবে পরবর্তী পর্বে।

ওয়েব ব্রাউজ করতে ব্রাউজার ব্যবহার করা জরুরী, কেনোনা ব্রাউজারই সেই টুল যেটা ওয়েবের সাথে আপনাকে কানেক্ট করে। ব্রাউজারকে এমন একটি পোর্টাল হিসেবে ধরতে পারেন, যেটা দুনিয়ার যেকোনো ওয়েবসাইটের সাথে আপনার কম্পিউটারকে কানেক্ট করে, সার্ভারকে রিকোয়েস্ট করে, সার্ভার থেকে ডাটা লোড করে। ব্রাউজার নিরাপদ রাখা অত্যন্ত গুরুত্বপূর্ণ ব্যাপার, তাই অবশ্যই হয়তো ব্রাউজার নিয়মিত আপডেটেড রাখেন, এবং ত্রুটি পূর্ণ এক্সটেনশন ব্যবহার করা থেকে বিরত থাকেন। কিন্তু তারপরেও ব্রাউজার সহজেই হ্যাক হয়ে যেতে পারে, আর সত্যি বলতে এখানে আপনাকে কোন

অ্যাকশন করারও দরকার পড়বে না, মানে কোন সাইটে গিয়ে কিছু না করে জাস্ট সাইট লিঙ্ক ক্লিক করেই আপনার ব্রাউজারকে অ্যাটাকের টার্গেট বানানো সম্ভব। আর দুর্ভাগ্যবশত অনেক অ্যান্টিভাইরাস পর্যন্ত এটি ডিটেক্ট করতে পারে না।

এথিক্যাল হ্যাকিং ফ্রী কোর্সের এই পর্বে আমি আলোচনা করবো ব্রাউজার হ্যাক নিয়ে। আজকে আলোচনা করা হবে ব্রাউজার হ্যাক কিভাবে হয়ে থাকে, কি কি তথ্য চুরি করতে পারে হ্যাকার এই হ্যাক এর মাধ্যমে? কিভাবে আপনি এই হ্যাক থেকে মুক্ত থাকতে পারবেন। তাহলে চলুন বেশি কথা না বলে শুরু করা যাক।

ব্রাউজার হ্যাক কি ও কিভাবে হয়ে থাকে?

ব্রাউজার হ্যাক খুব ভয়ংকর একটা পদ্ধতি, এই হ্যাক গুলো করা হয়ে থাকে Beef attack এর মাধ্যমে। আপনি যদি Beef Attack করতে চান তাহলে আপনার কম্পিউটারে অবশ্যই কালি লিনাক্স ইন্সটল করা থাকতে হবে [নেক্সট পর্বে কালি লিনাক্স ইন্সটল করার সম্পূর্ণ নির্দেশিকা দেখানো হবে!]। কালি লিনাক্স ছাড়া এই এট্যাক করা সম্ভব না। এই এট্যাক গুলো করা হয়ে থাকে হ্যাকার কোন ওয়েব পেজ বানিয়ে সেটার মাঝে একটা জাভা স্ক্রিপ্ট ফাইল দিয়ে রাখে, সেই লিঙ্কে আপনি শুধু একবার ঘুরে আসবেন। বাস আপনার আর কোন কাজ নেই, আপনি হ্যাক হয়ে গেছেন। এখন আপনি যেটাই করবেন আপনার ব্রাউজারে সেটাই হ্যাকার তার পিসি থেকে মনিটর করতে পারবে।

এখানে আসলে কাজ টা হয় কালি লিনাক্সে একটা টুল আছে Beef নামে আর সেটার নাম অনুসরে নাম করা হয়েছে Beef Attack। সেই টুল দিয়ে হ্যাকার পেলোড জাভা স্ক্রিপ্ট বানাই, সাথে তার জন্য একটা প্যানেল বানিয়ে নেয়। যেন হ্যাকার তার সেই প্যানেল থেকে সব কিছু মনিটর করতে পারে। সেই প্যানেলটা হয় গ্রাফিক্যাল, এবার হ্যাকার ওয়েব সার্ভারে একটা Html ফাইল বানাই আর সেটার সাথে পেলোড জাভা স্ক্রিপ্টটা সংযুক্ত করে দেয়। এবার ভিক্টিম কে সেই লিঙ্ক টা পাঠিয়ে দিল আর ভিক্টিম সেই লিঙ্কে গেল কিন্তু কিছুই পেল না। এবার সে ঘুরে চলে আসলো কিন্তু কিছুই বুঝতে পারলো না সে, আসলে সে যে হ্যাক হয়েছে তার কোন ধারনাই নেই। এবার ঢুকার সাথে সাথে হ্যাকারের কাছে

ইনফরমেশন চলে যাই, তখন হ্যাকার আপনার ব্রাউজারের নিয়ন্ত্রন পেয়ে যায়। আর এই ভাবেই ব্রাউজার হ্যাকটা হয়ে থাকে। এ থেকে বাঁচতে এই আর্টিকেলটি অত্যন্ত গুরুত্বপূর্ণঃ ম্যালিসিয়াস লিঙ্ক ক্লিক না করেই কিভাবে বুঝবেন এটি নিরাপদ কিনা?

ব্রাউজার হ্যাক করে কি তথ্য পাওয়া সম্ভব?

ব্রাউজার হ্যাক করে হ্যাকার আপনার ব্রাউজার থেকে কি কি তথ্য পেতে পারে? এখন তো প্রশ্ন এটাই তাই না ভাই? আসলে দেখেন হ্যাকার হ্যাক তো করেই তথ্য গুলো নেয়ার জন্য তাই না? এখানেও কিন্তু হ্যাকার অনেক তথ্য পেয়ে থাকে। ব্রাউজার হ্যাক করে একটা ব্রাউজারের সকল কিছুই নিয়ন্ত্রন করা সম্ভব। আপনি ক্রোম ব্যবহার করেন বা ফায়ারফক্স সকল ব্রাউজারে এটা তথ্য চুরি করতে পারে। নিম্নে দেয়া হল কি কি তথ্য হ্যাক হয়ে থাকে ব্রাউজার হ্যাকিং এর মাধ্যমে;

হুক সাইট বা ব্রাউজারে সেভ করা সাইট গুলো। আপনি কি কি সাইতে ব্রাউজ করেছেন সেটার লিস্ট হ্যাকার পেয়ে যাবে।কুকিজ চুরি করতে পারে। মানে আপনি ব্রাউজারে কোন সাইটে কিভাবে লগইন হয়ে রয়েছেন, সকল সেশন চুরি হয়ে যাবে। হ্যাকারকে নতুন করে পাসওয়ার্ড দিয়ে সাইটে লগইন করতে হবে না। মনে করুণ আপনি ফেসবুকে লগইন করে রেখেছেন, ব্যাস হ্যাকারের কম্পিউটারেও আপনার ফেসবুক আইডি অটো লগইন হয়ে যাবে।

আপনার কম্পিউটারে কমন কি কি সফটওয়ার ইন্সটল করা আছে সেটার লিস্ট পেয়ে যাবে। যেমন ধরুন আপনি মাইক্রোসফট অফিস ব্যাবহার করেন এবার আপনি হ্যাক, হ্যাকার বুঝতে পারবে আপনি মাইক্রোসফট অফিস ব্যবহার করেন, হতে পারে আপনার ভার্সনে কোন ত্রুটি রয়েছে, আর সেভাবেও অ্যাটাক করে দেবে।LastPass নামে একটা এক্সট্রেনশন আছে সেটা থেকে তথ্য চুরি করা সম্ভব। বলে রাখা ভাল এখন সব থেকে জনপ্রিয় পাসওয়ার্ড ম্যানেজার হচ্ছে LastPass তাহলে বুঝতেই পারছেন কতটা ঝুকিতে সবাই। যদিও এতে ডাটা গুলো এনক্রিপ্ট করা থাকে, তবে সেগুলোকে ডিক্রিপ্ট করাও সম্ভব।আপনার ব্রাউজারের টুল বার ও বুকমার্ক থেকে সকল তথ্য চুরি করা

সম্ভব।আপনার ওয়েবক্যাম চালু বা বন্ধ করে দিতে পারবে।তাছাড়া এটার সব থেকে বড় ব্যাপার হচ্ছে আপনাকে সাইট ফরওয়ার্ড করে ফিসিং সাইট বা অন্য সাইটেও নিয়ে যেতে পারে, আবার আপনার কম্পিউটারে পেলোড ডাউনলোডের জন্য আপনাকে বার বার ফোর্স করতে পারে এটা। মানে ব্রাউজার দিয়ে আপনি অ্যাড্রেস টাইপ করে যেতে চাইবেন গুগলে, কিন্তু চলে যাবেন হ্যাকারের ফেক সাইটে, আর আপনার ব্রাউজার কম্পিউটারে আর নতুন নতুন ম্যালওয়্যার গুলোকে আমন্ত্রণ জানাবে।এটা আপনাকে ফেক লগইন করাতে জোর করাতে পারে, যেমন আপনি ফেসবুক চালাচ্ছেন এই সময় পপআপ লগইন অপশন উঠেছে, বলছে আপনার সেশন শেষ পুনরায় লগইন করুন। আপনি তো কিছুই না বুঝে সেই পপ-আপ লগইন আপশনে লগইন করে রেখে দিবেন। আর ব্যাস, পাসওয়ার্ডটা চলে গেলো ভোগে, তাই অবশ্যই টু-ফ্যাক্টর ভেরিফিকেশন চালু করে নেওয়া অত্যন্ত গুরুত্বপূর্ণ। এতে হ্যাকার আপনার পাসওয়ার্ড চুরি করার পরেও আপনার আইডি লগইন করতে পারবে না।

এমন অনেক কিছু করা যায় যার শেষ আমার লেখার মাধ্যমে করা সম্ভব না। এর ব্যস্তব ব্যবহার তো প্র্যাক্টিক্যাল করে দেখানো সম্ভব নয়, তাহলে সেটা সম্পূর্ণ ব্ল্যাকহ্যাট হ্যাকিং হয়ে যাবে। এই অ্যাটাক কিভাবে করতে হয় সেটা নিচে শিখিয়ে দিচ্ছি। তবে অবশ্যই এথিক্যাল ভাবে একে ব্যবহার করতে হবে, অবশ্যই কারো উপর অ্যাটাক করতে পাড়বেন না, অবশ্যই পারমিশন নিতে হবে। এখন এখানে আরেকটি প্রশ্ন রয়েছে, একজন এথিক্যাল হ্যাকারের এরকম হ্যাক অ্যাটাক সম্পর্কে জেনে কাজ কি? দেখুন, আপনি একজন সিকিউরিটি স্পেশালিষ্ট, এর মানে আপনাকে ব্ল্যাকহাটেরও বাপ হতে হবে। হতে পারে কম্পিউটার ব্রাউজার সিকিউরিটি চেক করার জন্য বা ইন্টারনেট সিকিউরিটি সফটওয়্যার ঠিকভাবে কাজ করছে কিনা সেটা দেখার জন্য আপনাকে এরকম অ্যাটাক চালাতে হতে পারে। তবে অবশ্যই সেটা কারো বিরুদ্ধে চালানো যাবে না।

Beef Attack কিভাবে করবেন?

বিফ অ্যাটাক করার জন্য দুইটি ধাপ রয়েছে, প্রথমত আপনাকে নিজের

লোকাল সিস্টেম কনফিগার করতে হবে এবং দ্বিতীয়ত আপনি যে বা যার ব্রাউজার হ্যাক করতে চান সেই ব্রাউজারকে হুক করতে হবে। বিসয়টি অনেকটা এমন যে, ঐ ব্রাউজারে একটি ট্র্যাকিং ডিভাইজ লাগিয়ে দেওয়া, যেটি সর্বদা সকল ডিটেইলস গুলোকে আপনার পর্যন্ত পৌছাতে থাকবে। BeEF মূলত কালি লিনাক্সের বিল্ডইন টুল, তাই একে নতুন করে ডাউনলোড বা ইন্সটল করার প্রয়োজন পড়বে না।

স্টার্ট বিফ

বিফ টুলটির একটি গ্রাফিক্যাল ইন্টারফেস থাকে, যার মাধ্যমে আপনি সকল বিষয় গুলোকে মনিটর করতে পাড়বেন। তো প্রথমে আপনার সিস্টেম রেডি করতে হবে। তাহলে এক নজরে দেখে নেওয়া যাক, এই অ্যাটাকে আমাদের কি কি লাগছে।

অবশ্যই একটি কম্পিউটার অথবা রাসবেরি পাইকালি লিনাক্স অপারেটিং সিস্টেমআপনার ইন্টারনেট কানেকশন এবং নেটওয়ার্কে সকল পোর্ট ওপেন থাকতে হবে (পোর্ট ওপেন করা পোর্ট স্ক্যান করা নিয়ে পরবর্তী পর্বে বিস্তারিত আলোচনা করা হবে)মাথা ঠাণ্ডা রাখতে হবে, এবং কাজে ফোকাস প্রদান করতে হবে।

এবার আপনার কম্পিউটারে বিফ টুল রান করিয়ে সেটাকে কনফিগ করে নেওয়ার পালা। আপনি দুই ভাবে বিফ টুল রান করতে পাড়বেন। যেহেতু এটি একটি অ্যাপ্লিকেশন, তাই “Applications” -> “Kali Linux” -> “System Services” -> “BeEF” -> “beef start.” — এখানে গেলেই বিফ টুল রান হয়ে যাবে। আবার চাইলে কালি লিনাক্স টার্মিনাল ওপেন করে “cd /usr/share/beef-xss
./beef” এই কম্যান্ড প্রবেশ করানোর মাধ্যমেও বিফ টুলটি রান করতে পাড়বেন।

ব্যাস, বিফ টুল রান করানোর মাধ্যমে আপনার কম্পিউটারে প্রয়োজনীয় সকল সার্ভিস রান হয়ে যাবে এবং আপনার কন্ট্রোল প্যানেলও তৈরি হয়ে যাবে। আপনার লোকাল হোস্টে (127.0.01) যেকোনো ব্রাউজার ব্যবহার করে আপনার কন্ট্রোল প্যানেল অ্যাক্সেস করতে পাড়বেন। বিফ কন্ট্রোল প্যানেলটি

3000 পোর্টে ওপেন হয়। তাই প্যানেলে প্রবেশ করার জন্য নিচের অ্যাড্রেসটি ব্রাউজারে টাইপ করুণ।

http://localhost:3000/ui/authentication

এরপরে একটি লগইন পেজ ওপেন হবে এবং আপনাকে প্যানেলে লগইন করতে হবে। ডিফল্টভাবে ইউজারনেম এবং পাসওয়ার্ড হচ্ছে “beef” — ব্যাস ক্রেডিনশিয়াল প্রবেশ করানোর সাথে সাথে আপনি এই পাওয়ার টুলে প্রবেশ করে ফেলতে পাড়বেন এবং যেকোনো ওয়েব ব্রাউজার হ্যাক করতে পাড়বেন। আর এখানেই আপনার হ্যাক করা মানে আক্রমণ করা ব্রাউজার গুলোর তালিকা প্রদর্শিত হবে।

ব্রাউজার হুকিং

এই টুলের মূল উদ্দেশ্য হচ্ছে আপনাকে অবশ্যই ভিক্টিমের ব্রাউজার হুক করতে হবে। মানে ব্রাউজারে এমন একটি কোড লোড করিয়ে দিতে হবে যাতে ব্রাউজার সকল তথ্য আপনার পর্যন্ত সেন্ড করতে থাকে। সাধারণত কোন ওয়েব সার্ভারে হুক কোডটি ইন্সটল করে রাখতে হবে, হতে পারে সেটা আপনার নিজের ওয়েসাইটে বা হতে পারে যেকোনো ওয়েবসাইট যেটা আপনি নিয়ন্ত্রন করতে পাড়বেন। এবার আপনার ভিক্টিমকে ঐ সাইটে প্রবেশ করাতে হবে, সোশ্যাল ইঞ্জিনিয়ারিং ব্যবহার করিয়ে আপনার লিঙ্কে তাকে প্রবেশ করাতে হবে, এবার জাস্ট আক্রান্ত সাইটটি ওপেন করার সাথে সাথেই ব্রাউজারটিতে হুক কোড ইনজেক্ট হয়ে যাবে।

বিফ হুক মূলত একটি জাভা স্ক্রিপ্ট ফাইল, যেটার নাম সাধারণত “hook.js” হয়ে থাকে। ভবিষ্যৎ টিউটোরিয়ালে দেখাবো কিভাবে হুক ফাইল তৈরি করতে হবে, এবং কিভাবে বিভিন্ন উপায়ে ভিক্টিমের ব্রাউজারে হুক ফাইল ইনজেক্ট করে দিতে পাড়বেন। তারপরে বিস্তারিত জানিয়ে দেবো, কিভাবে আপনি ওয়েবপেজে এই জাভা ফাইলটি অ্যাড করতে পাড়বেন।

আমি আমার লোকাল নেটওয়ার্কে থাকা একটি কম্পিউটার ব্রাউজারকে হুক করেছি, দেখতেই পাচ্ছেন এটা ইন্টারনেট এক্সপ্লোরার ৬ যেটা পুরাতন

উইন্ডোজ এক্সপি ওএস এর উপর রান করছে। তো একবার আপনি কারো ব্রাউজার সফলভাবে হুক করতে সক্ষম হলে আপনি অনেক টাইপের ম্যালিসিয়াস অ্যাক্টিভিটি চালাতে পাড়বেন। অনেক টাইপের কম্যান্ড সেখানে রান করাতে পাড়বেন এবং অনেক তথ্য হাতিয়ে নিতে পাড়বেন। আসলে হুক করা ব্রাউজারের সাথে কতো কিছু করানো সম্ভব। তবে এসমস্ত ডিটেইল টিউটোরিয়াল পরের পর্ব গুলোতে আসবে, কেনোনা এখনো অনেক বিষয় পরিষ্কার করা বাকী আছে। আপনাদের পোর্ট সম্পর্কে ভালো ধারণা দিতে হবে। ওয়েব সার্ভারে ফাইল ইনজেক্ট করা শেখাতে হবে, লিনাক্স ইন্সটল থেকে শুরু করে বেসিক ইন্টারফেস নিয়ে আলোচনা করতে হবে। এই পোস্টটি জাস্ট একটি ডেমো পোস্ট বলতে পারেন, এ থেকে আপনি ধারণা নিতে পাড়বেন আসলে আপনি এই কোর্স থেকে পরবর্তীতে কিরকম অ্যাডভান্স বিষয় জানতে এবং প্র্যাকটিক্যাল শিখতে পাড়বেন। তবে অবশ্যই এই বিষয়টি ১০০% সম্পূর্ণ করেই শেখানো হবে, কিন্তু একটু ধৈর্য ধারণ করতে হবে।

কিভাবে আপনার ব্রাউজারকে হ্যাকার থেকে মুক্ত রাখবেন?

এবার চলে আসি আমাদের আসল ব্যবসায়, মানে অবশ্যই একজন এথিক্যাল হ্যাকার হিসেবে যেমন আপনার যেকোনো অ্যাটাক কিভাবে করতে হয় সে সম্পর্কে জ্ঞান থাকতে হবে, অনুরুপভাবে অবশ্যই সেই অ্যাটাক ঠেকাতে কি করতে হবে সেটার স্পষ্ট জ্ঞান চাই। যদিও এই অ্যাটাক ভয়াবহ সব কর্মকাণ্ড করতে সক্ষম, কিন্তু এটি ঠেকানো কিন্তু একেবারেই সাধারণ কাজ। আর সবুজ বাংলা ইউটিউব হেল্পলাইন এই গ্রুপে এই টাইপের সিকিউরিটি নিয়ে অনেক আলোচনা করা হয়েছে।

প্রথমত, অবশ্যই আপনার ইন্টারনেট ব্রাউজার এবং যেকোনো ইন্টারনেট টুলকে সর্বদা লেটেস্ট ভার্সনে আপডেট করে রাখতে হবে। আপনার অপারেটিং সিস্টেম সর্বদা আপডেটেড রাখতে হবে, ডাটা খরচ করার কানজুসি দেখাতে গিয়ে যে, উইন্ডোজ আপডেট বন্ধ করে রাখবেন সেটা করা যাবে না, না হলে পরিনাম কি হতে পারে বুঝতেই তো পাড়ছেন।

অবশ্যই অচেনা এবং অপরিচিত ব্রাউজার এক্সটেনশন ইন্সটল করবেন না,

কেবল অফিশিয়াল ওয়েবসাইট থেকে এক্সটেনশন ডাউনলোড করবেন। সাথে অ্যাড ব্লকার ব্যবহার করতে হবে, এতে ম্যালিসিয়াল স্ক্রিপ্ট গুলো রান হবে না। আর এখানে সবচাইতে গুরুত্বপূর্ণ ধাপ হলো, অবশ্যই আপনার পাসওয়ার্ড গুলো ব্রাউজারে সেভ করে রাখবেন না। কেনোনা সেগুলো সহজেই পেয়ে যাওয়া সম্ভব হবে, লাস্টপাস পাসওয়ার্ড ম্যানেজার ব্যবহার করা উত্তম হবে, কেনোনা এতে সকল ডাটা এনক্রিপটেড করানো থাকে—এবং পরিশেষে অবশ্যই ভিপিএন ব্যবহার করবেন, এতে আপনার কম্পিউটারের আসল আইপি অ্যাড্রেস কখনোই হ্যাকার পাবে না, তার কাছে টেম্প আইপি যাবে, যেটা থেকে সে পরবর্তী সময়ে ডিস্কানেক্ট হয়ে যাবে।

আশা করছি, এই সম্পূর্ণ পোস্ট থেকে ওয়েব ব্রাউজার হ্যাক করার সম্পূর্ণ ধারণা পেয়ে গেছেন এবং কিছু বিষয় তো এখানে প্র্যাকটিক্যাল বুজানো হয়েছে। পরবর্তী কোন পর্বে ব্রাউজার হ্ককিং করা শেখানো হবে, কিন্তু তার আগে আরো অনেক কিছু জানতে হবে, যার সম্পর্কে আরো বিস্তারিত নেক্সট পর্ব গুলোতে আলোচনা করা হবে। যেহেতু এটি এথিক্যাল হ্যাকিং কোর্স তাই অবশ্যই বিষয় গুলোকে নৈতিক কাজেই ব্যবহার করতে হবে, অবশ্যই সিস্টেমকে সিকিউরিটি দিতে হবে, কাউকে হ্যাক করা আমাদের কাজ না। নেক্সট পর্বে, আরো অসাধারণ কিছু নিয়ে হাজির হবো, সেই পর্যন্ত সবাই ভালো থাকবেন। আর যদি ভালো লাগে তাহলে অবশ্যই এই পোষ্টে লাইক প্রদান করে কমেন্ট বক্সে আপনাদের মূল্যবান মতামত প্রদান করবেন।

এথিক্যাল হ্যাকিং ফ্রী কোর্সঃ পর্ব - ০৬; ইমেইল স্পুফিং বৃত্তান্ত!এথিক্যাল হ্যাকিং ফ্রী কোর্স এর পর্ব ০৬ এ আপনাকে স্বাগতম। অনেক দিন পরে আজ শুরু করলাম এথিক্যাল হ্যাকিং পর্ব ০৬ এর লেখা। আজ আমি আপনাদের সাথে আলোচনা করবো ইমেইল স্পুফিং নিয়ে, এর নাম হয়তো অনেকে শুনে থাকবেন আবার অনেকে না শুনে থাকতেও পারেন। তবে সম্যসা নাই আপনি যদি শুনে থাকেন ইমেইল স্পুফিং নিয়ে তবে সেটা ভাল, আর যদি না শুনে থাকেন তবে সেটা ব্যাপার না। আমি আজ এর সকল বিষয় গুলো নিয়ে বিস্তারিত ভাবে বুঝিয়ে বলবো। আগেই বলে রাখি ইমেইল স্পুফিং কে কেও সহজ ভাবে নিবেন না। হতে পারে এটা খুব সহজ পদ্ধতি কিন্তু ইন্টারনেটে সব

থেকে ভয়ংকর বিষয় এটি। এখন পৃথীবিতে যত ক্রেডিট কার্ড ও পেপাল একাউন্ট হ্যাক হয় তার ৭৫% শুধু মাত্র এই ইমেইল স্পুফিং করে হয়ে থাকে। তাহলে বুঝতেই পারছেন আপনার অনলাইন একাউন্ট সুরক্ষিত রাখার জন্য এটা জানা কতটা জরুরি।তাহলে চলুন আর কথা না বাড়িয়ে শুরু করা আজকের আলোচনা।

ইমেইল স্পুফিং কি?

ইমেইল স্পুফিং নিয়ে যদি আলোচনা করতেই হয়, সবার আগে আলোচনা করতে হবে ইমেইল স্পুফিং কি এইটা নিয়ে। ইমেইল স্পুফিং হচ্ছে কারো কাছে মিথ্যা ইমেইল পাঠানো। কি বুঝতে পারলেন না? আচ্ছা ধরুন আপনার কাছে আমি আপনার বাবার ইমেইল ব্যবহার করে ইমেইল পাঠালাম। সেই ইমেইলে লিখে দিলাম কালকেই তুমি বাসায় চলে আসো। কিন্তু আপনার বাবা আপনার কাছে এই নিয়ে কোন ইমেইল পাঠায় নি। এটা অনেক টা আপনার কাছে মিথ্যা চিঠি পাঠানোর মত, কেও একজন আপনার ঠিকানায় ইচ্ছাকৃত ভুল চিঠি পাঠাচ্ছে। এবার মানে বুঝতে পারলেন? ইমেইল স্পুফিং আসলে কি! একে স্পুফিং বলার মূল কারণ হচ্ছে, আপনার কাছে অবিকল একই রকম দেখতে মেইল অ্যাড্রেস থেকে ইমেইল পাঠানো হয়। যদি অ্যাড্রেস আলাদা হয়, তাহলে ফেইক মেইল চেনা অনেক সহজ, কিন্তু একই অ্যাড্রেস থেকে আসা মেইল বুঝতে পারা একটু মুশকিলের, বেশিরভাগ মানুষই সহজেই এই স্পুফ করা মেইলের কবলে পড়ে যায়।

স্পুফ করা মেইলে কিন্তু শুধু মেইল অ্যাড্রেসই স্পুফ করা হয় না, মেইলটি কোথা থেকে এসেছে, মেইলকারীর নাম, মেইল অ্যাড্রেস, রিপ্লাই করলে মেইলটি সাধারণত আরেক মেইল অ্যাড্রেসে চলে যায়। তাছাড়া মেইল স্পুফিং করার সময় সার্ভার আইপি অ্যাড্রেস ও নকল করা হয়, সত্যি বলতে কোন এক্সপার্ট যদি মেইল স্পুফ করে, সেটা বোঝা অনেকবেশি কস্টের ব্যাপার হয়ে যায়, যতোক্ষণ পর্যন্ত আপনি ঐ আসল ব্যাক্তিকে কল করে জিজ্ঞাস না করেন, সে মেইল পাঠিয়েছে কিনা।

কারা ইমেইল স্পুফিং করে এবং কেন?

ইমেইল স্পুফিং মূলত করে থাকে হ্যাকারেরা (ব্ল্যাক হ্যাট হ্যাকার), কিন্তু এদের বলা হয়ে থাকে স্প্যামার। এদের কে এই জন্যই স্প্যামার বলা হয়ে থাকে কেননা এরা আসলে যে মেইল গুলো পাঠিয়ে থাকে সেই গুলো স্প্যাম মেইল। এরা আসলে এই কাজ গুলো করে থাকে তাদের স্বার্থ হাসিল এর জন্য। এখন প্রশ্ন আসতে পারে তাদের আবার কি স্বার্থ আছে এখানে? তাদের এটাই স্বার্থ যে তারা কিছু টাকা নিতে পারে মিথ্যা কথা বলে। এই বিষয় টা নিয়ে একটু বেশি বুঝিয়ে বলি। স্প্যামার'রা এই ইমেইল স্পুফিং করে আপনার ইন্টারনেট এর যে কোন আইডি হ্যাক করতে পারে। কিন্তু সব থেকে বেশি তাদের টার্গেট থাকে ব্যাংক একাউন্ট, ক্রেডিট কার্ড, পেপাল একাউন্ট ও বিভিন্ন ই-ব্যাংক একাউন্ট এর দিকে। তারা কিছু ইমেইল খুজে বের করে এবং সেই সব ইমেইল গুলোতে আসলে কিসের একাউন্ট খোলা আছে সেই গুলো সহ বের করে। তারা অনেকটা ডিজিটাল মার্কেটারের মত করেই ইমেইল গুলো বের করে থাকে। তাছাড়া অনেক টুল আছে এই গুলো চেক করার জন্য, যা এখানে বলা সম্ভব না। এরপরে সেই সব মেইল গুলোতে তারা স্প্যাম মেইল পাঠায়, হয়তো কারো কাছে পাঠায় কম্পানির মেইল ব্যবহার করে। এটা আসলে মূলত একটা অভিজ্ঞতার ব্যাপার আর কি। আর এই সব মেইল গুলো পাঠানোর জন্য অনলাইনে অনেক টুল রয়েছে, তাছাড়া হ্যাকার নিজেও ওয়েব সার্ভার ব্যবহার করে ইমেইল টুল বানিয়ে থাকে। যদিও এখন ওয়েব সার্ভার ব্যবহার করা হয়ে থাকে, এটা আসলে আপডেট ভার্সন।

তবে শুধু ফিশিং বা কার্ড হ্যাকিং এর জন্যই কিন্তু মেইল স্পুফিং ব্যবহৃত হয় না, হ্যাকারের প্ল্যান আরো খারাপ এবং আর বিধ্বংসী হতে পারে। বিশেষ করে হ্যাকার আপনার সিস্টেমে র‍্যাটওয়্যার ছড়ানোর জন্যও ফেইক মেইল পাঠাতে পারে, এখানে ফেইক মেইল পাঠালে বেশি সাকসেস হওয়ার সম্ভবনা থাকে, কেনোনা আপনি হয়তো মেইল অ্যাড্রেসটিকে বিশ্বাস করবেন এবং অজান্তে ভাইরাস ফাইলটি ডাউনলোড করবেন। তাছাড়া অনেক ম্যাস-মেইলিং ওয়র্মস থাকে, যেগুলো আপনার অ্যাড্রেস বুক রীড করতে পারে, মানে আপনার সকল কন্টাক্ট গুলোতে স্বয়ংক্রিয়ভাবে ফেইক মেইল পাঠাতে আরম্ভ করবে, হ্যাকার শুধু আপনাকে নয়, এভাবে আপনার সকল কন্টাক্ট মেইল গুলোকেও আক্রান্ত করানোর চেষ্টা করতে পারে।

হ্যাকার'রা কিভাবে কারো ইমেল খুজে পায়?

এখন প্রশ্ন এসে দাড়াচ্ছে হ্যাকার কিভাবে আপনার বা আমার ইমেইল খুজে পায়? এর আগে আমি একটা আমার সাথে ঘটে যাওয়া একটা ঘটনা বলি, হয়তো এটা শোনার পরে আপনার মনের প্রশ্নের উত্তর পেয়ে যাবেন। গত ২০১৫ তে শেষের দিকে আমি একটা ওয়েব সাইট খুলবো বলে সিদ্ধান্ত নিলাম কিন্তু আমার কাছে তো কোন কার্ড ছিল না তাই বাইরের দেশের কোন কোম্পানির কাছে থেকে হোস্টিং কিনতে পারলাম না, তাই কিনলাম আমার দেশের নাম করা একটা কোম্পানির কাছে থেকে, আমি এখানে কাওকে ছোট করছি না, আসলে এই কাজ টা এখন সারা পৃথিবীর সকলেই করে থাকে। যায় হোক কেনার পরে ৩-৪ দিন পরে বাংলাদেশের আরেকটা বড় কোম্পানির কাছে থেকে আমার কাছে ইমেইল এসেছে, তাদের হোস্টিং এ –৫০% ছাড় চলছে, সাথে ছোট করে লেখা আছে আমি নাকি তাদের ওয়েবসাইট এ সাবস্ক্রাইব করেছি। কিন্তু আমি তো তাদের ওয়েবসাইটেই যায়নি। এর মানে কি? তারা আমার ইমেইল কোথায় পেয়েছে? একটু ভাবুন!! কি? ভেবে পেলেন?

আসলে আমি যেই ওয়েবসাইট থেকে হোস্টিং কিনেছি সেই ওয়েবসাইট আমার ইমেইলটা অন্য ওয়েবসাইট এর কাছে বিক্রি করে দিয়েছে। তাহলে একটু ভাবুন তো এই ইমেইল যদি কোন হ্যাকার কিনে থাকে তাহলে তার ফলাফল কি হতে পারে? এখন কি বুঝতে পেরেছেন হ্যাকার আপনার বা আমার ইমেইল কিভাবে পেয়ে থাকে? তারা আসলে ইমেইল লিস্ট কিনে থাকে, তাছাড়া তারা আরো অনেক পন্থা ব্যবহার করে থাকে। যেমন বিভিন্ন নিউজ লেটার ব্যবহার করে আপনার বা আমার ইমেইল কালেক্ট করে থাকে। এছাড়াও তারা কিছু বট ব্যবহার করে থাকে, যেই বট গুলো তাদের অটোমেটিক ইমেইল সংগ্রহ করে দেয়। গুগল বট বা ফেসবুকের অনেক বট আছে, আসলে ভাল কাজের জন্য থাকে বট গুলো। কিন্তু এইসব বট গুলোর খারাপ ব্যবহার হয় আর কি। আসলে এই বট গুলো কাজ করে থাকে কোন ওয়েব পেজে @ এই টা খোজার মাধ্যমে। কোন ওয়েব সাইটে যদি আপনার ইমেইলটা কোন ভাবে টেক্সট আকারে থেকে থাকে তাহলে জেনে রাখুন আপনি জেনে শুনে হ্যাকারকে আপনার মেইল তার হাতে তুলে দিয়েছেন। তাই ভুল করেও কোন ওয়েবসাইটের কমেন্ট সেকশনে

নিজের মেইলটি কমেন্ট আকারে পাবলিশ করবেন না। যদি কমেন্ট সেকশনে মেইলের আলাদা বক্স থাকে, যেখানে প্রবেশ করাতে পারেন, কেনোনা ঐটা প্রটেকটেড হয়ে থাকে।

কিভাবে মেইল স্পুফিং করবেন (এডুকেশন্যাল)

কেও এটাকে খারাপ ভাবে নিবেন না, ভেবেছিলাম কোন প্রাকটিক্যাল বলবো না। কিন্তু হ্যাকিং এ যদি প্রাকটিক্যাল না দেখানো বা না বলা হয় তাহলে কেমন যেন লাগে। তাহলে চলুন জেনে নেই কিভাবে ইমেইল স্পুফিং করবেন? আপনি ইমেইল স্পুফিং এর জন্য অনেক টুল পেয়ে থাকবেন, কিন্তু বর্তমানে সব থেকে বেশি ব্যবহার করা হয় ওয়েব সার্ভার টুল। আমি নিজেও ওয়েব সার্ভার ব্যবহার করে ইমেইল স্পুফিং করে থাকি। এর জন্য আপনার লাগবে শেল, শেল বলতে একটা PHP ফাইল। এই শেল টাকে আপনি আপনার অথবা আপনার হ্যাক করা সার্ভারে আপলোড করে দিন আর মজা নিন। আপনি ইন্টারনেটে WSO নামে একটা শেল পাবেন, এই শেল টাতে আপনি ইমেইল স্পুফিং করার অপশন পাবেন। আজকের এই পোস্টে আমি এই শেল গুলো শেয়ার করতে পারছি না। কারণ যদি আমি এই পোস্টটিতে এইই শেলগুলি শেয়ার করি তাহলে এই পোস্টটা কে ফেসবুক কর্তৃপক্ষ স্পাম হিসেবে নেবে এবং একটি কমিউনিটি গাইডলাইন স্ট্রাইক প্রদান করবে। যদি কারো খুব দরকার পরে থাকে তাহলে আমার সাথে কন্টাক্ট করতে পারেন।আপনাদের বিশেষ প্রয়োজনে প্রাইভেট ভাবে যোগাযোগ করলে আমি সম্পূর্ণ পদ্ধতি শিখিয়ে দিতে পারবো, সিকিউরিটির জন্য সবুজ বাংলা ইউটিউব হেল্পলাইন গ্রুপে এরকম টিউটোরিয়াল ওপেন করে দেওয়া সম্ভব নয়, তবে আপনি চাইলে গুগল করেও কিভাবে শেল সেটআপ করে নিতে হয় তা শিখে ফেলতে পারেন, শেলের নাম তো দিয়েই দিলাম, এখন আপনি ভালো করেই জানেন আপনাকে কি লিখে সার্চ করতে হবে!

এবার আপনি এই টুলের ব্যবহার করে যেকোনো মেইল হুবহু তৈরি করে ভিকটিমকে পাঠাতে পারবেন। তো বুঝলেন তো, কিভাবে সহজেই হ্যাকার আপনাকে একেবারে হুবহু আসল মেইল অ্যাড্রেসের মতো অ্যাড্রেস থেকে মেইল সেন্ড করতে পারে। যদি আপনি সার্ভার সেটআপ না করতে চান,

সেক্ষেত্রে বিভিন্ন অনলাইন টুল রয়েছে, যেখানে মেইল অ্যাড্রেস হুবহু ডুপ্লিকেট করে মেইল সেন্ড করতে পাড়বেন, অনেক সার্ভিস হয়তো ফ্রী অনেকের কাছে হয়তো সার্ভিস প্ল্যান কিনতে হয়, তবে যদি আপনার কাছে একটি ওয়েব সার্ভার থাকে, সহজেই এরকম টুল বানানো সম্ভব। চলুন, নিচে আমাকে কমেন্ট করে জানিয়ে দিন, যদি ভালো রেসপন্স পাই, আপনাদের ফ্রী ওয়েব সার্ভারে মেইল স্পুফিং সেটআপ গাইড পিডিএফ বানিয়ে আপনাদের মাঝে শেয়ার করবো।

ফেক মেইল চেনা ও এর প্রতিকার।

সব সম্যসার আসলে একটা সমাধান থাকে, এখন কথা হচ্ছে আমরা কিভাবে ইমেইল স্পুফিং থেকে নিজেকে রক্ষা করবো। আমি কিন্তু আগে থেকে একটা কথা খুব ভালভাবে বলে আসছি সতর্ক থাকুন। কেননা ইন্টারনেটে সতর্ক থাকা ছাড়া অন্য কোন উপায় খুব কম কাজ করে থাকে। তারপরেও কিছু কিছু বিষয় তো থাকে সেই গুলোও আমি বলবো চিন্তা করবেন না। আসলে হ্যাকার'রা অনেক সময় এমন এমন ইমেইল পাঠায় যে মনে হয় আসলে এটা সত্য ইমেইল। কিন্তু মনে রাখবেন আপনার কাছে আপনার ব্যাংক বা ই-ব্যাংক কোন সময় পাসওয়ার্ড পরিবর্তন করতে বলবে না বা আপনার ইনফোরমেশন পূনরায় দিতে বলবেনা। যদিও বা দিতে বলে থাকে তাহলে আপনি যেই ওয়েব সাইটে যাচ্ছেন সেই ওয়েব সাইটের URL ভালভাবে দেখে নিন। খুব ভাল ভাবে বানান গুলো দেখে নিন, যদি দেখেন সব ঠিক আছে তাহলে আপনি দিতে পারেন, আর যদি দেখেন না ভুল দেখাচ্ছে কিছু একটা, তাহলে এই ইমেইল থেকে দূরে থাকুন। এ ছাড়া আপনার কাছে যে ইমেইল টা আসছে সেই মেইল টা কোথায় থেকে আসছে, এর SMTP সার্ভার কি সেটা ভালভাবে দেখে নিন।

আপনারা আপনাদের জিমেইল একাউন্টের স্প্যাম মেইলের স্প্যামবক্সে ভালো করে লক্ষ্য করুন আপনাদের কাছে কিভাবে স্প্যাম মেইল আসছে? আপনারা আপনাদের জিমেইল এর স্পাম বক্স এর স্প্যাম মেইল গুলো যদি দেখেন তাহলে খুব সহজেই আপনারা স্প্যাম মেইল দেখলেই খুব সহজে বুঝবেন কোনগুলো স্প্যাম মেইল। আশা করি এই সব বিষয় গুলো খেয়াল রাখলে আপনি সুরক্ষিত থাকতে পারবেন। আর আবারো বলছি, মেইলে থাকা লিঙ্কে ক্লিক করার আগে হাজারো বার ভেবে নিন, সাথে জেনে রাখুন, কিভাবে এসমস্ত মেলিসিয়াস

মেইল-এ ক্লিক না করেই বুঝবেন আপনি নিরাপদ কিনা এই সম্পর্কিত একটি পোস্ট আমি পরবর্তীতে আপনাদের জন্য নিয়ে আসছি।

ইমেইল বোম্বিং

ভাবতে পারেন এটা তো আজকে কথা ছিল না ভাই। দিলাম ভাই আজ একটু বেশি এমনিতেই অনেকদিন লেখা দেইনি, যদি একটু বেশি না দেই, তাহলে কি হয়? আপনি কি এই নাম টা শুনেছেন? হয়তো শুনেছেন। আর যদি না শুনে থাকেন এর নাম শুনে হয়তো বুঝতেই পারছে এটা হবেই সেই রকম একটা জিনিস। আসলে ইমেইল বোম্বিং হচ্ছে কোন ইমেইলে এক সাথে অনেক ইমেইল পাঠানো। কিন্তু ভুলেও ভাবেন না এটা একটা ইমেইল থেকেই পাঠায়, এটা অনেক মেইল থেকে পাঠায়!

ইমেইল বোম্বিং এর মধ্যে হ্যাকারের অনেক গভীর স্বার্থ লুকিয়ে থাকতে পারে। আপনাকে আগেই বলে রাখি, যখন কোন হ্যাকার বা হ্যাকার টিম বড় টাইপের হ্যাকিং করার চেষ্টা করে, সেক্ষেত্রে ভিক্টিমের প্রত্যেকটি বিষয়ের উপর নজর রাখা হয়। অনেক সময় কারো বিজনেস ডাউন করার জন্যও হ্যাকার মেইল বোম্বিং করতে পারে। ধরুন, আপনার এক বিশেষ কোম্পানির সাথে বিশেষ ডিল হতে চলেছে এবং একটি মেইল আসতে পারে সে ব্যাপারে, আর আপনাকে ঐ মেইলের অবশ্যই রিপ্লাই করতে হবে, যদি আপনি ডিলটি ফাইনাল করতে চান। এখন মনে করুণ, কোন হ্যাকার বা আপনার প্রতিদ্বন্দ্বী আপনার সকল বিষয়ের উপর গভীর নজর রেখেই চলছে, সেক্ষেত্রে ঠিক কাজের মেইলটি আসার পূর্বের মুহূর্তে আপনাকে ১ লাখ মেইল সেন্ড করে দেওয়া হবে। এতে আপনার ইনবক্স ফুল হয়ে যাবে, আপনি নতুন মেইল পাবেন না, বা নতুন মেইল আসলেও সেটা এক বিশাল পরিমান মেইলের ব্ল্যাকহোলে হারিয়ে যাবে।

এবার কথা হচ্ছে এই মেইল বোম্বিং কিভাবে থামাবেন? আপনার যেই মেইল আসছে সেই মেইলটাকে সিলেক্ট করে স্প্যাম বক্সে দিয়ে দিন। বাস শেষ, এবার হ্যাকার ব্যাটা মুড়ি খেয়ে বেড়াক। কিভাবে আপনি মেইল বোম্বিং করবেন, ওয়েল, গুগল করুণ, অনেক টিউটোরিয়াল পেয়ে যাবেন ফ্রী'তে! এখানে আলোচনা করলাম না, কেনোনা বিষয়টি আজকের টপিক এর জন্য তেমন

গুরুত্বপূর্ণ নয়। আর এরকম ব্যাপার নিয়ে যতোই বলি “কেউ খারাপ কাজে ব্যবহার করবেন না” । কিন্তু ৮০%ই মানুষ খারাপ কাজেই ব্যবহার করবে।

পরিশেষে আমি একটা কথায় বলবো নিজের উপস্থিত বুদ্ধি কাজে লাগিয়ে অনেক বড় বড় অ্যাটাক থেকে বেঁচে যেতে পারেন, সেটা অনলাইন/অফলাইন। ইমেইল স্পুফিং খুব ভয়ানক মেথড যেকোন অনলাইন আইডি হ্যাক হবার জন্য। আশা করি আমার আজকের এইই এথিক্যাল হ্যাকিং ফ্রী কোর্স ০৬ আপনার ভাল লেগেছে। সবুজ বাংলা ইউটিউব হেল্পলাইন এবং আমি সবুজ চাই আপনারা নিজের সুরক্ষা যেন আপনি নিজে দিতে পারেন, আর সেই লক্ষে আমার এই ক্ষুদ্র প্রচেষ্টা। একজন এথিক্যাল হ্যাকার হিসেবে আপনাকে সচেতনা সৃষ্টি করতে হবে, আপনাকে বা আপনার ক্ল্যায়েন্ট’কে বিষয় গুলো বুঝিয়ে দিতে হবে। সাথে অনেক মহৎ কাজ করার জন্য হয়তো আপনাকেও বিভিন্ন টেকনিক ব্যবহার করতে হতে পারে। একজন পরিপূর্ণ এথিক্যাল হ্যাকার বা সিকিউরিটি স্পেশালিষ্ট হিসেবে নিজেকে তৈরি করার জন্য আপনাকে ব্ল্যাক হ্যাটেরও বাপ রুপে নিজেকে তৈরি করতে হবে। কিন্তু সেই ব্ল্যাক হ্যাট হ্যাকার এর বাবা হিসাবে নিজেকে তৈরি করতে গেলে ধীরেসুস্থে ধৈর্য ধারণ করে ইথিক্যাল হ্যাকিং শিখতে হবে। এক লাফে গাছে ওঠা যাবে না।,আস্তে আস্তে ধীরে সুস্থে শিখতে হবে, কিন্তু আমাদের মাঝে বেশিরভাগ লোকেরই সে ধৈর্যটা নেই আর যাদের ধৈর্যটা নেই তারা কখনোই কোন ধরনের হ্যাকিং শিখতে পারবে না। তো তাহলে আজ এই পর্যন্তই পরবর্তী ইথিক্যাল হ্যাকিং কোর্স আপনাদের জন্য নিয়ে আসছি প্র্যাকটিক্যাল একটি আকর্ষণ, সেই পোস্টের জন্য অপেক্ষা করুন। আর আজকের এই পোস্টটি কেমন হয়েছে তা অবশ্যই আপনারা কমেন্ট বক্সে জানাবেন কারণ আপনাদের লাইক শেয়ার এবং কমেন্ট এর মাধ্যমে পরবর্তী পোস্ট দেওয়ার জন্য আমি আরো অনেক বেশি অনুপ্রেরণা পাই।