আইক্লাউড হলিউড সেলিব্রেটির ফটো হ্যাক ও ব্রুট ফোর্স অ্যাটাক

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

২০১৪ সালের ৩১ আগস্ট হলিউডের বিভিন্ন সেলিব্রেটির প্রায় ২০০ একান্ত ব্যক্তিগত ছবি, যার বেশিরভাগই মহিলা এবং অনেকগুলো আবার নগ্ন– এগুলো ইমেজবোর্ড চ্যানেল ৪ এ পোস্ট করা হয়। পরবর্তী সময়ে অন্য ব্যবহারকারীরা এগুলো অন্যান্য ওয়েবসাইট, সামাজিক নেটওয়ার্ক, যেমন– ইমগুর, রেডিট ও টাম্বলার ইত্যাদিতে ছড়িয়ে দেয়।

ধারণা করা হয়, অ্যাপল ক্লাউড সার্ভিস 'সুইট আইক্লাউড'-এর মাধ্যমে ছবিগুলো সংগ্রহ করা হয়। অ্যাপল পরে নিশ্চিত করে, ইমেজগুলো অ্যাকাউন্ট ইনফরমেশন হ্যাক করার মাধ্যমে সংগ্রহ করা হয়েছে, যা খুব সুনির্দিষ্টভাবেই আক্রমণ করা হয়েছে, যেমন– পাসওয়ার্ড সংগ্রহ করা ইত্যাদি। এটি আইক্লাউডের কোনো নিরাপত্তার ভঙ্গুরতা নয়।

যদিও অ্যাপল আনুষ্ঠানিকভাবে স্বীকার করেনি, কিন্তু সবার ধারণা– হ্যাকগুলো ঘটে ছিল অ্যাপল আইফোনের 'ফাইন্ড মাই আইফোন' নামের ফিচারের ভালনারেবিলিটি ব্যবহার করে। 'আই-ব্রুট' ভালনারেবিলিটি ফাইন্ড মাই আইফোন ওয়েবসাইটে আনলিমিটেড পাসওয়ার্ড অ্যাটেম্পটের মাধ্যমে করা হয়, যা লকড করা হয়নি। লগইন অথেনটিকেশনের জন্য এ ধরনের আনলিমিটেড অ্যাটাক হ্যাকার সমাজে 'ব্রুট ফোর্স অ্যাটাক' নামে পরিচিত। এ লেখায় আলোচনা হয়েছে কীভাবে এ ধরনের আক্রমণ করা হয় এবং কীভাবে তা থেকে নিজেদেরকে রক্ষা করা যায়।

ব্রুট ফোর্স অ্যাটাক

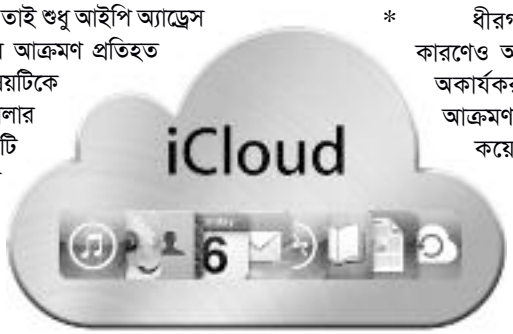
ব্রুট ফোর্স অ্যাটাক কোনো ওয়েবসাইটের অ্যাক্সেস পাওয়ার জন্য সবচেয়ে সাধারণ একটি উপায় বেছে নেয়। ইউজারনেম ও পাসওয়ার্ডের মাধ্যমে এটি বারবার চেষ্টা করতে থাকে, যে পর্যন্ত না চেষ্টা সফল হয়। যদিও এটি খুব সাধারণ মনে হয়, তবুও এটি বেশ কার্যকর যখন লোকেরা ১২৩৪৫৬ টাইপের পাসওয়ার্ড এবং অ্যাডমিনের মতো ইউজারনেম ব্যবহার করে। সংক্ষেপে এটি হলো কোনো ওয়েবসাইটের নিরাপত্তা ব্যবস্থার সবচেয়ে দুর্বলতম লিঙ্কে আক্রমণ করা।

এ ধরনের আক্রমণের ফলে ওয়েবসাইটের সার্ভারে মেমরি ঘাটতি দেখা দেয় এবং স্বাভাবিক কার্যক্রমে সমস্যা সৃষ্টি করে। এর কারণ, আপনার ওয়েবসাইটে এত উচ্চহারে এইচটিটিপি অনুরোধ আসতে থাকে (অর্থাৎ ওয়েবসাইটে কোনো ভিজিটরের বারবার ভিজিট করার কারণে) যে, সার্ভারের মেমরি ঘাটতি দেখা যায়।

কোনো একজন আক্রমণকারী সবসময়ই কাঙ্ক্ষিত পাসওয়ার্ড পেয়ে যায়, কিন্তু তা হতে বছরের পর বছর লেগে যেতে পারে (!) পাসওয়ার্ডের দৈর্ঘ্য এবং জটিলতার ওপর নির্ভর করে ট্রিলিয়নসংখ্যক সম্ভাব্য কম্বিনেশন হতে পারে। এটি আরও একটু সহজে করার জন্য ডিকশনারির শব্দগুলোর মতো বা শব্দগুলো কিছুটা পরিবর্তন করে চেষ্টা করা হয়। কারণ, বেশিরভাগ লোকই একবারে এলোপাতাড়ি কোনো শব্দ ব্যবহার করতে চায় না, বা করে না। এ ধরনের আক্রমণকে ডিকশনারি অ্যাটাক বা হাইব্রিড ব্রুট ফোর্স অ্যাটাক্ট বলা হয়।

আমরা কীভাবে নিরাপদ থাকতে পারি

হ্যাকাররা ব্রুট ফোর্স অ্যাটাক শুরু করে ব্যাপকভিত্তিক ব্যবহৃত টুল ব্যবহার করেই, যা শব্দতালিকা এবং স্মার্ট রুলসেটস ব্যবহার করে। এটি অতন্ত বুদ্ধিমত্তা এবং স্বয়ংক্রিয়ভাবে ইউজারের পাসওয়ার্ড অনুমান করে থাকে। এ ধরনের আক্রমণ খুব সহজেই শনাক্ত করা যায়, কিন্তু সহজে প্রতিরোধ করা যায় না। উদাহরণ, অনেক এইচটিটিপি ব্রুট ফোর্স টুল ওপেন প্রক্সি সার্ভার তালিকার মাধ্যমে রিকোয়েস্ট রিলে করতে পারে। যেহেতু প্রতিটি রিকোয়েস্ট ভিন্ন ভিন্ন আইপি অ্যাড্রেস থেকে আসে, তাই শুধু আইপি অ্যাড্রেস ব্লক করেই এ ধরনের আক্রমণ প্রতিহত করা সম্ভব নয়। বিষয়টিকে আরও জটিল করে তোলার জন্য কিছু টুল প্রতিটি অ্যাটেম্পটে আলাদা আলাদা ইউজার নেম ও পাসওয়ার্ড দিয়ে চেষ্টা করে। কাজেই ফেইল্ড



পাসওয়ার্ড অ্যাটেম্পটকে ব্লক করেও এটি প্রতিহত করা সম্ভব নয়।

অ্যাকাউন্ট লক করা

এ ধরনের ব্রুট ফোর্স অ্যাটাককে প্রতিহত করার সবচেয়ে অবশ্যম্ভাবী উপায় হলো, একটি নির্দিষ্ট সংখ্যক ভুল পাসওয়ার্ড অ্যাটেম্পটের পরপরই অ্যাকাউন্টটি ব্লক করে দিতে হবে। অ্যাকাউন্টটি একটি নির্দিষ্ট সময়ের জন্য লক করে দেয়া যায়, যেমন– এক বা দুই ঘণ্টা অথবা একজন অ্যাডমিন ম্যানুয়্যালি আনলক করা পর্যন্ত অ্যাকাউন্টটি লক করা থাকবে। যাই হোক, অ্যাকাউন্ট ব্লক করে দেয়া সবসময় কোনো উত্তম সমাধান নয়। কেননা, যেকেউই নিরাপত্তার এ ব্যবস্থাকে অপব্যবহার করতে পারে এবং শত শত ইউজারের অ্যাকাউন্ট লক করে রাখতে পারে। বস্তুত কিছু কিছু ওয়েবসাইট এত বেশি আক্রমণের শিকার হয় যে কর্তৃপক্ষ এই লক আউট পলিসি প্রয়োগ করতে পারছে না। এতে অনবরত কাস্টমারের অ্যাকাউন্ট আনলক করতে হচ্ছে।

অ্যাকাউন্ট লকআউট করার সমস্যাগুলো নিম্নরূপ

* আক্রমণকারী অনেকগুলো অ্যাকাউন্ট লক আউট করে ডিনায়্যাল অব সার্ভিসের (DoS) কারণ হতে পারে।
* কারণ, অস্তিত্বহীন কোনো অ্যাকাউন্ট লক আউট করা যায় না, শুধু ভ্যালিড অ্যাকাউন্ট নামই লক করা য়ায়। আক্রমণকারী এ বিষয়টি ব্যবহার করে সাইট থেকে ইউজার নেম সংগ্রহ করতে পারে এরর রেসপন্সের ওপর ভিত্তি করে।
* অনেকগুলো অ্যাকাউন্ট লক আউট করে আক্রমণকারী ডাইভারশন তৈরি করতে পারে এবং সাপোর্ট কলের মাধ্যমে হেল্প ডেস্ককে ভাসিয়ে ফেলতে পারে।
* আক্রমণকারী অনবরত একই অ্যাকাউন্ট লক আউট করতে পারে, এমনকি অ্যাডমিনিস্ট্রেটর আনলক করার সেকেন্ডের মধ্যেই, যা কার্যকরভাবে অ্যাকাউন্টটি ডিজ্যাবল করতে পারে।
* ধীরগতির আক্রমণের কারণেও অ্যাকাউন্ট লক আউট অকার্যকর হয়, যেখানে আক্রমণকারী প্রতিঘণ্টায় শুধু কয়েকবার চেষ্টা করে থাকে।
* ইউজার নেমের একটি দীর্ঘ তালিকার জন্য শুধু একটি পাসওয়ার্ড ব্যবহার করে, আক্রমণের কারণেও অ্যাকাউন্ট লক আউট অকার্যকর হয়।
* ইউজার নেমে/পাসওয়ার্ডের একটি কম্বো লিস্ট দিয়ে আক্রমণ করলে এবং প্রথম কয়েকটি অ্যাটেম্পটেই সঠিক অনুমান করতে পারে, তাহলেও অ্যাকাউন্ট লক আউট অকার্যকর হয়।
* শক্তিশালী অ্যাকাউন্ট যেমন– অ্যাডমিনিস্ট্রেটর অ্যাকাউন্টে সাধারণত লক আউট পলিসি বাইপাস করা থাকে, কিন্তু দুর্ভাগ্যবশত এ অ্যাকাউন্টগুলো আক্রমণের জন্য খুবই আকর্ষণীয় হয়ে থাকে। কিছু সিস্টেমে অ্যাডমিনিস্ট্রেটর অ্যাকাউন্ট লক আউট করা হয় শুধু নেটওয়ার্ক ভিত্তিক লগ ইনের জন্য।
* এমনকি আপনি যদি অ্যাকাউন্ট লক আউটও করেন, এরপরও আক্রমণ চলতেই পারে, যা মূল্যবান মানবসম্পদ ও কমপিউটার রিসোর্সেস কনজিউম করে থাকে।

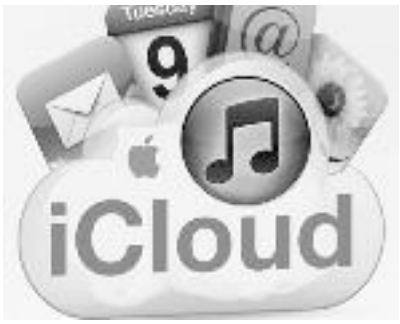
অ্যাকাউন্ট লক আউটও কোনো কোনো ক্ষেত্রে কার্যকর হতে পারে, কিন্তু এটি হতে পারে শুধু নিয়ন্ত্রিত পরিবেশে অথবা ওই সব ক্ষেত্রে, যেখানে ঝুঁকিমুক্ত থাকা এতটাই গুরুত্বপূর্ণ যে, এমনকি অ্যাকাউন্টস কম্প্রোমাইজের চেয়ে নিরবচ্ছিন্ন ডিনায়্যাল অব সার্ভিস (DoS) আক্রমণও বেশি গ্রহণযোগ্য। যাই হোক, ▸

বেশিরভাগ ক্ষেত্রে ব্রুট ফোর্স অ্যাটাক্ট ঠেকাতে অ্যাকাউন্টস লক আউট যথেষ্ট নয়। উদাহরণ, কোনো অকশন সাইট যেখানে একই আইটেমের জন্য কয়েকজন বিডার দর কষাকষি করছে। এখন যদি অকশন ওয়েবসাইট লক আউট সিস্টেম প্রয়োগ করে, তাহলে যেকোনো বিডার শেষ মুহূর্তে অন্য বিডারদের অ্যাকাউন্ট লক করে উইনিং বিড সাবমিট করা থেকে বিরত রেখে সহজেই বিডটি জিতে নিতে পারে। একই টেকনিক প্রয়োগ করে একজন আক্রমণকারী ক্রিটিক্যাল অর্থনৈতিক লেনদেন বা ই-মেইল যোগাযোগ বন্ধ করে দিতে পারে।

ইনজেকশন র‍্যান্ডম পজেস ইন অথেনটিকেশন

আগে যেমন আলোচনা করা হয়েছে অ্যাকাউন্ট লক আউট সাধারণত কোনো বাস্তব সমাধান নয়, কিন্তু ব্রুট ফোর্স অ্যাটাক ঠেকাতে অন্যান্য উপায়ও রয়েছে। প্রথমত, আক্রমণকারী সফল হওয়া না হওয়া নির্ভর করে সময়ের ওপর, তাই একটি সহজ সমাধান হলো পাসওয়ার্ড চেক করার সময় একটি র‍্যান্ডম পজ ইনজেক্ট করা। এমনকি কয়েক সেকেন্ড পজ যোগ করেও আক্রমণকে অনেক অনেক স্লো করে দেয়া যায়, কিন্তু বৈধ ব্যবহারকারীকে যা মোটেই বিরক্তির মধ্যে ফেলে না।

মনে রাখতে হবে, র‍্যান্ডম পজেস পদ্ধতি একক থ্রেড সহজেই স্লো করতে পারলেও



আক্রমণকারী যদি একই সাথে মাল্টি-অথেনটিকেশন অনুরোধ পাঠায়, তবে এটি অপেক্ষাকৃত কম কার্যকর হয়ে থাকে।

একটি আইপি অ্যাড্রেস লক আউট

আরও একটি সাধারণ সমাধান হতে পারে, একটি আইপি অ্যাড্রেস লক করা হবে যদি অ্যাড্রেসটি মাল্টিপল লগইন ফেইল্ড করে। এ সমাধানের একটি সমস্যা হলো, আপনি অসতর্ক বা ভুলবশত কোনো আইএসপি বা বড় কোম্পানির ব্যবহৃত প্রক্সি সার্ভার ব্লক করার মাধ্যমে বিপুলসংখ্যক ব্যবহারকারীর আইপি বন্ধ করে দিতে পারেন। অন্য আরও একটি সমস্যা হলো, অনেক টুল প্রক্সি লিস্ট ব্যবহার করে থাকে এবং অন্যটিতে মুভ করার আগে প্রতিটি আইপি অ্যাড্রেস থেকে শুধু কয়েকটি অনুরোধই পাঠিয়ে থাকে।

গোপন প্রশ্ন

একটি বা দুটি লগইন ফেইল্ড হলে আপনি একটি গোপন প্রশ্নের উত্তর চাইতে পারেন। এটি শুধু অটোমেটেড আক্রমণই প্রতিহত করে না। এটি আক্রমণকারীকে অ্যাক্সেস গ্রহণ করতেও প্রতিহত করে। এমনকি ব্যবহারকারীর সঠিক পাসওয়ার্ড ও ইউজার নেম জানা সত্ত্বেও। আপনি সিস্টেমে আক্রমণের উচ্চমাত্রা সম্পর্কেও জানতে পারবেন এবং এর ভিত্তিতে সিস্টেমের সব ইউজারের গোপন প্রশ্নের উত্তর দেয়া বাধ্যতামূলক করা না করার সিদ্ধান্তও নিতে পারবেন।

নির্দিষ্ট আইপি অ্যাড্রেস থেকে লগইন

অগ্রণী বা গুরুত্বপূর্ণ ব্যবহারকারীদেরকে আক্রমণের হাত থেকে রক্ষার জন্য শুধু একটি নির্দিষ্ট আইপি অ্যাড্রেস থেকে লগইনের অপশন রাখা যেতে পারে।

ক্যাপচার ব্যবহার

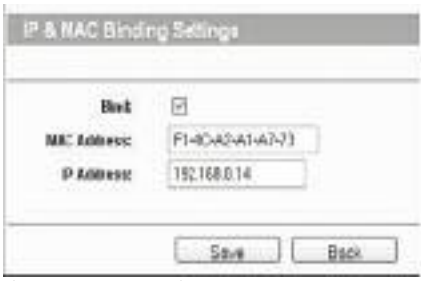
ব্রুট ফোর্সসহ সব ধরনের অটোমেটেড আক্রমণ থেকে বাঁচার অন্যতম সেরা উপায় হলো ক্যাপচার ব্যবহার। এটি এমন এক পরীক্ষা, যা মানুষের জন্য পাস করা সহজ হলেও কমপিউটারের জন্য সহজ নয় কজ

ফিডব্যাক : jabedmorshed@yahoo.com

ম্যাক অ্যাড্রেসের সাথে আইপি অ্যাড্রেস বন্ডিং

(৬৫ পৃষ্ঠার পর)

এখন যে ডিভাইসের ম্যাক অ্যাড্রেসের সাথে আইপি অ্যাড্রেসটি বাইন্ড করতে চাচ্ছেন তা এখানে বাইন্ড অপশনটিতে টিক (চ) মার্ক দিয়ে ম্যাক অ্যাড্রেসের ঘরে ম্যাক অ্যাড্রেসটি ও আইপি অ্যাড্রেসের ঘরে আইপি অ্যাড্রেসটি টাইপ করে সেভ বাটনে ক্লিক করুন।

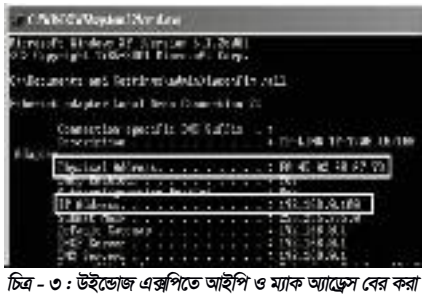


চিত্র -২ : ম্যাক ও আইপি অ্যাড্রেস বাইন্ড করা

ধাপ-৬ : কনফিগারেশনটি ঠিক থাকলে রাউটারটি একবার রিস্টার্ট দিন। এবার আপনার কাজ শেষ। এবার যে কমপিউটারকে বন্ডিং করেছেন, ওই কমপিউটারের আইপি অ্যাড্রেসটি পরিবর্তন করে দেখুন কমপিউটারে ইন্টারনেট ব্যবহার করতে পারবেন না। অর্থাৎ রাউটারে সেটআপ করা নির্দিষ্ট ম্যাক ও আইপি অ্যাড্রেস ম্যাচ করলেই আপনি ইন্টারনেট ব্যবহার করতে পারবেন।

কমপিউটারের ম্যাক অ্যাড্রেস বের করা

যেকোনো কমপিউটারের ম্যাক অ্যাড্রেস খুব সহজেই বের করা সম্ভব। ল্যান কার্ড রয়েছে এমন কোনো কমপিউটারে ম্যাক অ্যাড্রেস বের করতে হলে কমান্ড প্রম্পটে একটি কোড টাইপ করে এন্টার প্রেস করলে আইপি ও ম্যাক অ্যাড্রেসটি প্রদর্শিত হবে। বিষয়টি স্পষ্ট করার জন্য নিচের ধাপ দুটি দেখুন।



চিত্র - ৩ : উইন্ডোজ এক্সপিতে আইপি ও ম্যাক অ্যাড্রেস বের করা

০১. উইন্ডোজ এক্সপিতে ম্যাক অ্যাড্রেস বের করার জন্য স্টার্ট→রান→cmd টাইপ করে এন্টার চাপুন। এবার কমান্ড প্রম্পটে ipconfig/all টাইপ করে এন্টার চাপলে ওই কমপিউটারের ল্যান কার্ডের আইপি ও ম্যাক অ্যাড্রেসটি দেখতে পাবেন।

০২. লিনআক্স/উবুন্টুতে ম্যাক অ্যাড্রেস বের করার জন্য প্রথমে টার্মিনাল উইন্ডোটি চালু করতে হবে। এবার টার্মিনালে ifconfig/all টাইপ করে এন্টার চাপুন। এতে ওই অপারেটিং সিস্টেমে কত আইপি ও ম্যাক অ্যাড্রেস বসানো রয়েছে তা জানতে পারবেন।

সতর্কতা

ধরুন, আপনার নেটওয়ার্কে থাকা ৫০টি কমপিউটারের মধ্যে ৪০টি ম্যাক ও আইপি বন্ডিং করে দিয়েছেন। কিন্তু বাকি ১০টির ইউজাররা একটু চালাকি করলেই ইন্টারনেটের সাথে যুক্ত হতে পারবেন। তাই ম্যাক ও আইপি অ্যাড্রেস কারও সাথে শেয়ার করবেন না এবং থার্ড পার্টি সফটওয়্যার ব্যবহার করে কেউ যেনো ম্যাক অ্যাড্রেস ও কমপিউটারের আইপি বের করতে না পারে, সেদিকে লক্ষ রাখুন কজ

ফিডব্যাক : rony446@yahoo.com

জেনে নিন

ফেসবুকের শর্টকাট কি

Alt+1 = হোম পেজে যেতে
Alt+2 = নিজ প্রোফাইলে (ওয়াল) যেতে
Alt+3 = কে আপনাকে ফ্রেন্ড রিকোয়েস্ট পাঠাল তা চেক করতে (রিকোয়েস্ট না থাকলে কাজ করবে না)
Alt+4 = কে আপনাকে মেসেজ পাঠাল তা চেক করতে (মেসেজ না থাকলে কাজ করবে না)
Alt+6 = অ্যাকাউন্ট সেটিংসে যেতে
Alt+7 = অ্যাকাউন্ট প্রাইভেসিতে যেতে
Alt+8 = ফেসবুকের ফ্যান পেজে যেতে
Alt+0 = ফেসবুকের হেল্প সেন্টারে যেতে
Alt+m = নতুন মেসেজ লিখতে