যারা নতুন হ্যাকিং শিখতে চায় তাদের জন্য আমার কিছু কথা

যদি আপনি নতুন হ্যাকিং শিখতে আগ্রহী হন, তাহলে নিম্নলিখিত কিছু কথা আপনার জন্য উপকারী হতে পারে:

1. ভালো অনলাইন সংস্থান অনুসন্ধান করুন: হ্যাকিং বিষয়ে পর্যাপ্ত জ্ঞান অর্জনের জন্য ইন্টারনেটে ভালো সংস্থান অনুসন্ধান করুন। ব্লগ, ফোরাম, ওয়েবসাইট, অনলাইন কোর্স, ভিডিও টিউটোরিয়াল সহ বিভিন্ন উপায়ে লাভজনক তথ্য পেতে পারেন। এছাড়াও, হ্যাকিং সংক্রান্ত বই পড়াও আপনাকে সাহায্য করতে পারে।

2. কোর্স এবং ট্রেনিং প্রাপ্ত করুন: হ্যাকিং সংক্রান্ত বিভিন্ন অনলাইন কোর্স ও প্রশিক্ষণে অংশ নিতে পারেন। এই কোর্স এবং প্রশিক্ষণ প্রোগ্রামগুলি আপনাকে হ্যাকিং নিয়ে ভালো ধারণা দিবে এবং কাজে লাগাতে সহায়তা করবে।

3. প্রাকটিস করুন: হ্যাকিং শিখতে প্রাকটিস করা খুবই গুরুত্বপূর্ণ। একটি হ্যাকিং ল্যাব তৈরি করে নিজের উপর বিভিন্ন পরীক্ষা নিয়ে দেখুন এবং প্রাকটিস করুন। ভালো হ্যাকিং প্রাকটিস করার জন্য প্রয়োজনীয় কম্পিউটার সিস্টেম, সফটওয়্যার এবং প্রোগ্রামগুলি ইনস্টল করুন।

4. আইন ও নীতি সম্পর্কে জানুন: একটি ভালো হ্যাকার হওয়ার জন্য নৈতিক সাংগঠনিক দিক পালন করা খুবই গুরুত্বপূর্ণ। হ্যাকিং নিয়ে আইন ও নীতি জানা খুবই প্রয়োজন। হ্যাকিং কাজে নিজেকে নিয়ন্ত্রণ রাখার জন্য আইন এবং নীতিগুলি অবলম্বন করুন।

5. সাইবার সুরক্ষা সম্পর্কে জানুন: সাইবার সুরক্ষা হ্যাকিং এর একটি গুরুত্বপূর্ণ দিক। হ্যাকিং নিয়ে জ্ঞান অর্জনের পাশাপাশি, সাইবার সুরক্ষা বিষয়ে জানা অবশ্যই প্রয়োজন। সাইবার আক্রমণ, ডাটা লেকেজ, প্রাইভেসি নিয়ে জানুন এবং সাইবার সুরক্ষা উপায়ের ওপর কাজ করুন।

এগুলি মাত্র কেবলমাত্র কিছু উপায়। হ্যাকিং শিখতে সময় ও প্রচেষ্টা প্রয়োজন হবে। এছাড়াও, মানসিক স্থিতি ধরে রাখা ও ব্যক্তিগত আনুশাসন অবলম্বন করা উচিত। সহজ উপায়ে হ্যাকিং শিখতে যাওয়া অন্যতম পথ নয়, তবে পর্যাপ্ত ধৈর্য এবং প্রচেষ্টা দিলে আপনি কিছুদিনের মধ্যেই অন্ধকার থেকে প্রকাশের দিকে এগিয়ে যাবেন। শুভকামনা রইল।

সিকিউরিটি সিক্রেট হ্যাকবুক (Security Secrets HackBook)

এই বইটি পরলে আপনি হ্যাকিং সংক্রান্ত অনেক কিছুই শিখতে পারবেন। একজন প্রফেশনাল এথিকাল হ্যাকার হতে এই বইটি আপনকে সাহায্য করবে। বইটি পরে বেসিক থেকে শুরু করতে পারেন হ্যাকিং জগতের পথচলা।

- সম্পাদনায়
- নেহাল আহমেদ
- সাইবার সিকিউরিটি স্পেশালিষ্ট
- নীলফামারী, রংপুর বাংলাদেশ
- কন্টাক্ট নাম্বার +৮৮০১৬১৩০১৬৯৪৩

যেকোনো প্রয়োজনে কল করুন অথবা ফলো করুন আমাদের সামাজিক যোগাযোগ মাধ্যমে -

- ✓ Follow Me on Facebook : Nehal Ahmed
- ✓ Follow Me on Instagram : Nehal Ahmed
- ✓ Follow Me on Linkedin : Nehal Ahmed
- ✓ Follow Me on GitHub : Nehal Ahmed
- ✓ Call Me on WhatsApp : +8801613016943
- ✓ I Regularly write Articales : https://weirdnehal.blogspot.com/
- ✓ Visit My Website : http://weirdnehal.ezyro.com/

বিস্তারিত সুচিপত্রঃ

ইউনিট - ০১ : হ্যাকিং এর ভূমিকা ও বিশ্লেষণ

❖ অধ্যায় - ১.১ : হ্যাকার কাকে বলে?

হ্যাকার হলো কম্পিউটার সিস্টেম, নেটওয়ার্ক, সফ্টওয়্যার বা ওয়েবসাইটে অনধিকৃত অ্যাক্সেস পাওয়ার জন্য কোন ব্যক্তি। সাধারণত হ্যাকাররা বিভিন্ন কারণে নিজেদের কার্যক্রমের জন্য অনধিকৃত অ্যাক্সেস অর্জন করার চেষ্টা করে থাকেন। হ্যাকাররা সিস্টেমে নিরাপত্তা দুর্বলতা আবহাওয়া, সুরক্ষা বার্তা পাঠানো এবং সাইবার অপরাধের জন্য তারা নিরাপত্তা বিপর্যস্ত করে থাকেন।

হ্যাকারদের বিভিন্ন ধরণের হ্যাকিং প্রক্রিয়াগুলি থাকতে পারে, যেমন নেটওয়ার্ক হ্যাকিং, সিস্টেম হ্যাকিং, ওয়েবসাইট হ্যাকিং, পাসওয়ার্ড ক্র্যাকিং ইত্যাদি। কিছু হ্যাকার অপরাধীদের উদ্দেশ্য হতে পারে আর্থিক সাধারণত লাভ, তবে অন্যান্য কিছু হ্যাকাররা নৈতিক, রাজনৈতিক, গবেষণামূলক বা আর্থিক কারণে একটি সিস্টেম বা সেবা নিয়ে হ্যাক করেন।

তবে হ্যাকার শব্দটি সাধারণত নেতারাই ভীত এবং অপরাধীদের সংক্ষিপ্ত ধারণা দিয়ে উপস্থাপন করে। নিজেদের নিজস্ব কর্মকাণ্ডের উদ্দেশ্যে আপনার সিস্টেমে নিরাপত্তা পরীক্ষা করার জন্য আপনি নিরাপত্তা পেশা হ্যাকারদের কর্মসূচি ব্যবহার করতে পারেন, যা অনেক প্রাকৃতিক এবং প্রয়োজনীয় হতে পারে।

❖ অধ্যায় - ১.২ : হ্যাকার কত প্রকার ?

হ্যাকার বিভিন্ন প্রকারের হতে পারে, যা নিম্নলিখিত কিছুটা:

1. হ্যাকিং অপরাধী: এই প্রকারের হ্যাকাররা অননুমোদিত ও অসমর্থিত অ্যাক্সেস পেতে চেষ্টা করে সিস্টেম, নেটওয়ার্ক, সফ্টওয়্যার বা ওয়েবসাইটে। তারা সাধারণত প্রাণগ্রহণের জন্য এবং অপরাধিক উদ্দেশ্যে কাজ করে।

2. এথিক্যাল হ্যাকার: এই প্রকারের হ্যাকাররা সিস্টেমের নিরাপত্তা পরীক্ষা করে তার দুর্বলতা পরিষ্কার করে এবং সুরক্ষা বার্তা পাঠানোর জন্য কাজ করে। তারা সাধারণত সিকিউরিটি এজেন্ট, সিস্টেম অ্যাডমিনিস্ট্রেটর বা নেটওয়ার্ক পেনেট্রেশন টেস্টার হিসাবে কাজ করে।

3. সমাজসেবী হ্যাকার: এই প্রকারের হ্যাকাররা সাধারণত সাইবার অপরাধ দূর করার জন্য কাজ করে। তারা গভর্নমেন্ট, প্রতিষ্ঠান, বা সাধারণ ব্যক্তিদের সাইবার নিরাপত্তা বা অপরাধের জন্য পরামর্শ দেয়।

4. ক্র্যাকার: ক্র্যাকাররা সফ্টওয়্যার এবং ডিজিটাল পণ্যের প্রতিষ্ঠানিক নিরাপত্তা বার্তা পাঠাতে পারেন বা অনধিকৃত সফটওয়্যারের উন্নত বা কী প্রযুক্তি পেতে পারেন। কিছু ক্র্যাকাররা সফটওয়্যার পার্টিশন করতে পারেন বা লাইসেন্স কোড হ্যাক করতে পারেন।

উপরের তালিকায় উল্লিখিত হ্যাকার প্রকারগুলি মাত্র সাধারণ অবগতি প্রদান করার জন্য, বাস্তবিক সিদ্ধান্ত এবং হ্যাকারদের ব্যবহারের কারণগুলি বিবেচনা না করে। অনেক ক্ষেত্রে এই বিভাজনটি শারীরিক নয়, এখানে একটি হ্যাকার একাধিক ধরণের কাজ করতে পারে।

❖ অধ্যায় – ১.৩ : হ্যাকার কত ধরনের হতে পারে ?

হ্যাকার বিভিন্ন ধরণের হতে পারে এবং তারা বিভিন্ন উদ্দেশ্যে কাজ করে। নিম্নলিখিত কিছু প্রধান হ্যাকার ধরণগুলি রয়েছে:

1. নেটওয়ার্ক হ্যাকার: নেটওয়ার্ক হ্যাকাররা নেটওয়ার্ক ইনফ্রাস্ট্রাকচার, রাউটার, ফায়ারওয়াল, ডাটাবেস সার্ভার ইত্যাদির ক্ষেত্রে অনধিকৃত অ্যাক্সেস অর্জন করতে চেষ্টা করেন। তারা নেটওয়ার্কের ক্ষমতা, ডেটা পরিচর্যা, ব্যান্ডউইথ বা কানেকশনে দুর্বলতা তৈরি করতে পারেন।

2. সিস্টেম হ্যাকার: সিস্টেম হ্যাকাররা অনধিকৃত অ্যাক্সেস পেতে চেষ্টা করেন কম্পিউটার অপারেটিং সিস্টেম, সার্ভার, কার্যকর সিস্টেম সফটওয়্যার, ড্রাইভার ইত্যাদি এর মধ্যে। তারা কম্পিউটারের নিয়ন্ত্রণ অর্জন করতে পারেন, ফাইলগুলি পরিবর্তন করতে পারেন বা কম্পিউটারের কার্যক্রমে দুর্বলতা তৈরি করতে পারেন।

3. ওয়েব হ্যাকার: ওয়েব হ্যাকাররা ওয়েবসাইট, ওয়েব অ্যাপ্লিকেশন, ওয়েব সার্ভার বা ডেটাবেসে অনধিকৃত অ্যাক্সেস অর্জন করতে চেষ্টা করেন। তারা মালিকানাধীন ওয়েবসাইট হ্যাক করতে পারেন, ক্রয়-বিক্রয়ে দুর্বলতা তৈরি করতে পারেন, ব্যবহারকারীদের তথ্য অপহারণ করতে পারেন ইত্যাদি।

4. সাইবার অ্যাট্যাকার: সাইবার অ্যাট্যাকাররা সাইবার অপরাধ বা মালিকানাধীন কম্পিউটার সিস্টেমে হুমকি, হতাশা, অপসারণ বা ক্ষতি তৈরি করতে চেষ্টা করেন। তারা সাইবার পরামর্শ দেয়, এনক্রিপ্টেড তথ্য গ্রহণ করতে চেষ্টা করেন, সুরক্ষার দুর্বলতা অনুসন্ধান করেন ইত্যাদি।

এইগুলি কেবলমাত্র কিছু উদাহরণ এবং বিভিন্ন ধরণের হ্যাকার এর মধ্যে প্রধান একটি বিভাজন। সম্পূর্ণ হ্যাকার সমাজে পাওয়া যায় এবং তারা বিভিন্ন উদ্দেশ্যে কাজ করতে পারেন। অনেক হ্যাকার একই সময়ে একাধিক ধরণের কাজ করতে পারেন।

❖ অধ্যায় – ১.৪ : হ্যাকিং কিভাবে করা হয় ?

হ্যাকিং হলো কম্পিউটার সিস্টেম, নেটওয়ার্ক, সাইট, এ্যাপ্লিকেশন ইত্যাদির সুরক্ষা মেয়াদে অনধিকার প্রবেশ করার প্রয়োজনমূলক সুদর্শনের পদ্ধতি। হ্যাকিং বিভিন্ন পদ্ধতিতে করা হতে পারে এবং প্রতিষ্ঠানের নিরাপত্তা নিয়ে খেলাপী কাজ করতে ব্যবহার করা হয়।

একজন হ্যাকার অন্য ব্যক্তিদের গোপনীয় তথ্য, আর্থিক সম্পদ, ব্যবসায়িক তথ্য ইত্যাদি অন্ধকারে ছুঁড়ে দিতে পারে। নিচে কিছু হ্যাকিং পদ্ধতির উদাহরণ দেয়া হল:

1. পাসওয়ার্ড ক্র্যাকিং: হ্যাকাররা ব্যবহারকারীদের পাসওয়ার্ড অন্ধকারে আঁকার চেষ্টা করতে পারেন। এটি সাধারণত পাসওয়ার্ড দ্বারা লগইন সিস্টেমে প্রবেশের চেষ্টা করে। পাসওয়ার্ড ক্র্যাকিং পদ্ধতিতে হ্যাকাররা বিভিন্ন পাসওয়ার্ড ক্র্যাকিং টুল ব্যবহার করে অথবা রেইনবো হ্যাকিং টেকনিক ব্যবহার করে পাসওয়ার্ড ব্রুটফোর্স করে।

2. ফিশিং: হ্যাকাররা ম্যালিশাস ওয়েবসাইট, মেইল বা সামাজিক নেটওয়ার্ক পেজ তৈরি করে প্রতারকপ্রবেশ প্রাপ্ত করার চেষ্টা করতে পারেন। তাদের লক্ষ্য হল ব্যবহারকারীদের ব্যপারে ভুল ধারণা জনিত করে সংশয়ভাজন। সাধারণত এটি মেইল করে বা আনান্দপূর্বক সন্দেশ বা অফিশিয়াল লুকাপ হিসাবে উৎপন্ন করা হয়।

3. ম্যালওয়্যার: হ্যাকাররা আকাশপথে গ্রহণ করা অ্যাপস বা সফটওয়্যারের মধ্যে ম্যালওয়্যার প্রবেশ করার চেষ্টা করতে পারেন। এটি অন্ধকারে অতিক্রান্ত হয়ে গ্রহণযোগ্য পরিবেশ সৃষ্টি করতে পারে যাতে হ্যাকাররা অন্ধকারে নিরাপত্তা কম করে গুরুত্বপূর্ণ তথ্য স্থাপন করতে পারেন।

উপরের উল্লিখিত পদ্ধতিগুলি কেবলমাত্র উদাহরণ এবং কোনও ধূমপানকারী পদ্ধতির ব্যবহার একটি সাম্প্রতিকতার বিষয়। হ্যাকিং অন্যান্য পদ্ধতিগুলির মধ্যে উপরে উল্লিখিত নয়। এটি বিশেষ অনুমতি ছাড়াই অন্যদের সিস্টেমের ব্যবহার পরিবর্তন, তথ্য চুড়ান্ত করতে বা সন্দেহভাজন করতে পারে।

আমি জ্ঞাত করাতে চাই যে হ্যাকিং সম্পর্কিত অন্যান্য কাজের সাথে যুক্তিযুক্ত এবং বৈধ উপায়ে না। হ্যাকিং বা সাইবার আপরাধের প্রতিষ্ঠানগুলি ব্যবহার করা আইনত অবৈধ এবং নিয়মাবলী ভঙ্গের হিসাবে গণ্য করা হয়। অনুগ্রহ করে নীতিমালা ও আইনের মেয়াদে কম্পিউটার সিস্টেম এবং নেটওয়ার্ক সুরক্ষা সম্পর্কিত সঠিক অধ্যয়ন করে স্বচ্ছতামুলক ও নৈতিকতামূলক ব্যবহার করুন।

❖ অধ্যায় – ১.৫ : হ্যাকারদের জন্য ফোরাম ও রিসোর্স।

হ্যাকারদের জন্য অনেক ফোরাম এবং রিসোর্স রয়েছে, যেগুলি তাদের কাজে সহায়তা করতে পারে। নিম্নলিখিত কিছু ফোরাম এবং রিসোর্সগুলি রেফার করা হতে পারে:

1. HackerOne: HackerOne হ'য়েকারদের জন্য একটি প্ল্যাটফর্ম যা সাইবার নিরাপত্তা সমস্যার জন্য বোনাস ও প্রশাসনিক সমাধান সরবরাহ করে। এটি অন্তর্ভুক্ত কিছু জনপ্রিয় প্রতিষ্ঠানগুলির জন্য একটি বাগ বাগ প্রতিযোগিতায় অ্যাক্সেস প্রদান করে। এছাড়াও, এটি হ্যাকারদের জন্য মুদ্রণযোগ্য পাঠ্যকলা, রিসোর্স এবং যোগাযোগের সুবিধা প্রদান করে। লিংক: https://www.hackerone.com/

2. Null Byte: Null Byte হ'য়েকারদের জন্য একটি অনলাইন কমিউনিটি ও লার্নিং প্ল্যাটফর্ম। এখানে আপনি সাইবার সুরক্ষা, হ্যাকিং এবং কম্পিউটার নেটওয়ার্কের সমস্যার সমাধান এর বিভিন্ন বিষয়ে টিউটোরিয়াল, ব্লগ পোস্ট, বিভিন্ন উপাদান এবং অনলাইন ডিসকাশনের মাধ্যমে শেখার সুযোগ পাবেন। লিংক: https://null-byte.wonderhowto.com/

3. Reddit: Reddit হ'য়েকারদের জন্য একটি জনপ্রিয় অনলাইন কমিউনিটি যেখানে আপনি বিভিন্ন হ্যাকিং সংক্রান্ত সামগ্রী, ব্যবহারকারীদের পরামর্শ, টিউটোরিয়াল এবং ডিসকাশন পেতে পারেন। কিছু জনপ্রিয় হ্যাকিং সংক্রান্ত সাবরেডিটগুলি রয়েছে r/hacking, r/netsec, r/AskNetsec, r/HowToHack ইত্যাদি। লিংক: https://www.reddit.com/

4. OWASP: OWASP (Open Web Application Security Project) হ'য়েকারদের জন্য একটি গুরুত্বপূর্ণ সংস্থা যা ওয়েব অ্যাপ্লিকেশন সুরক্ষা এবং সাইবার নিরাপত্তার জন্য সংস্থানিক উন্নতি করে। এর ওয়েবসাইটে আপনি প্রকাশিত রিসোর্স, টিউটোরিয়াল, সামগ্রী এবং টুলসের সাথে সংযুক্ত হতে পারেন। লিংক: https://owasp.org/

এটি কেবলমাত্র কিছু উদাহরণ, আরো অনেক ওয়েবসাইট, ফোরাম এবং সাইবার নিরাপত্তার রিসোর্স রয়েছে যা হ্যাকারদের জন্য পাঠকের মধ্যে বিভিন্ন প্রশ্ন ও সমস্যার সমাধানে সহায়তা করতে পারে।

❖ অধ্যায় – ১.৬ : সোশ্যাল ইঞ্জিনিয়ারিং কি?

হ্যাকিং সোশ্যাল ইঞ্জিনিয়ারিং (Hacking Social Engineering) হল একটি কম্পিউটার হ্যাকিং প্রক্রিয়া যেখানে হ্যাকাররা মানুষের সামাজিক প্রশাসন, প্রতিষ্ঠানের নীতি ও নির্দেশিকা, সামগ্রিক বৈশিষ্ট্য এবং মানসিক প্রভাববান অংশগুলির ব্যবহার করে অতিক্রান্ত হয়ে প্রবেশ করার চেষ্টা করে।

হ্যাকিং সোশ্যাল ইঞ্জিনিয়ারিং অনেকগুলি পদ্ধতি ব্যবহার করে, যেমন খোলা তথ্য উদ্ভাবন, ধারণা সৃষ্টি, কমপ্যুটার ব্যবহারকারীকে প্রাপ্ত করা সামগ্রিক তথ্য, উদ্ভাবিত মঙ্গলগ্রহণ ও দ্বন্দ্বমূলকতা, মানসিক অবস্থার মতো উপাদানগুলির ব্যবহার ইত্যাদি। এই পদ্ধতিগুলির মাধ্যমে হ্যাকাররা সামাজিক প্রাণালীগুলির ক্ষেত্রে দুর্বলতা পাওয়া এবং সন্ত্রাসী প্রবেশের পথ প্রস্তুত করে। এর মাধ্যমে তারা সামগ্রিক গোপনীয়তা, আর্থিক তথ্য, ব্যক্তিগত তথ্য, ব্যবসায়িক তথ্য ইত্যাদি অধ্যয়ন করতে পারেন এবং উপযুক্ত পরিস্থিতিতে আপনার নিজের মতামত, ব্যাংকিং তথ্য, অ্যাকাউন্ট প্রমাণীকরণ তথ্য প্রাপ্ত করতে পারেন।

হ্যাকিং সোশ্যাল ইঞ্জিনিয়ারিং একটি মানুষ কে মানুষের সাথে জড়িত নয়, কিন্তু মানুষের ভূমিকা, সুপারিশ এবং প্রতিক্রিয়ার উপর ভিত্তি করে অতিক্রান্ত হয়ে যায়। এটি মানসিক দক্ষতা, সামাজিক সম্পর্ক, কম্পিউটার জ্ঞান ও নেটওয়ার্ক প্রকৌশলগুলির মিশ্রণে ভেদ করে।

উপরে উল্লেখিত পদ্ধতিগুলি একে একটি সামগ্রিক সামাজিক ইঞ্জিনিয়ারিং বা সামাজিক ইঞ্জিনিয়ারিং হ্যাকিং হিসাবে পরিচিত হয়।

ইউনিট – ০২ : হ্যাকিং করার সিস্টেম গুলো।

❖ অধ্যায় – ২.১ : ফিশিং?

ফিশিং অ্যাটাক হল একটি কারগর অনুপ্রাণিত হ্যাকিং পদ্ধতি যার মাধ্যমে হ্যাকাররা ব্যবহারকারীদের ব্যপারে ভুল ধারণা দেওয়া বা সংক্ষেপে আকর্ষণ প্রদান করে তাদের সামাজিক মাধ্যমিক অ্যাকাউন্ট, ইমেল, ব্যাংক অ্যাকাউন্ট তথা অন্যান্য গোপনীয় তথ্য প্রাপ্ত করে। ফিশিং অ্যাটাকে হ্যাকাররা সাধারণত মেল বা মেসেঞ্জারে আসা জালিয়াতি মেসেজ, যাতে প্রাপ্তবয়স্ক কার্যকর মেয়েদের ছবি ব্যবহার করা হয়, ব্যবহারকারীদের পাসওয়ার্ড পুনরাবৃত্তি করার অনুরোধ, ব্যবহারকারীর তথ্য আপডেট করার চেষ্টা করে তাদের সম্পদ উপস্থাপন করে। এই ধরনের অ্যাটাক কম্পিউটার নিরাপত্তা এবং ব্যবহারকারীর সতর্কতা প্রতিরোধ করতে বিভিন্ন পদক্ষেপ গ্রহণ করে।

❖ অধ্যায় – ২.২ : ব্রুটফোর্স অ্যাটাক?

ব্রুটফোর্স অ্যাটাক হল একটি কারগর হ্যাকিং পদ্ধতি যার মাধ্যমে হ্যাকাররা পাসওয়ার্ড অনুসন্ধানের জন্য বিভিন্ন কম্বিনেশনে পাসওয়ার্ড প্রদান করে দেখে একাউন্টে লগ ইন করার চেষ্টা করে। ব্রুটফোর্স অ্যাটাকে হ্যাকাররা সাধারণত কম্পিউটার প্রোগ্রাম ব্যবহার করে এই প্রক্রিয়াটি সহজলভ্য করে। নিম্নলিখিত ধাপগুলোতে ব্রুটফোর্স অ্যাটাক করা হয়:

1. প্রাথমিক কম্বিনেশনে পাসওয়ার্ড পরীক্ষা: হ্যাকাররা সাধারণত প্রাথমিক কম্বিনেশনে পাসওয়ার্ড পরীক্ষা শুরু করে যেমন সংখ্যা, বর্ণমালা, স্পেশাল ক্যারেক্টারগুলি ব্যবহার করে। এই পদ্ধতিতে সম্ভবত সক্ষমতার সর্বনিম্ন পরীক্ষামূলক পাসওয়ার্ডগুলি পরীক্ষা হয়।

2. পাসওয়ার্ড ডিকশনারি অ্যাটাক: হ্যাকাররা প্রযুক্তিগত পাসওয়ার্ড ডিকশনারিতে পাসওয়ার্ড অনুসন্ধান করতে পারেন। একটি পাসওয়ার্ড ডিকশনারি সাধারণত সাধারণ বা সম্ভব্য পাসওয়ার্ডগুলির একটি তালিকা যা সম্ভাব্যতা অনুযায়ী পাসওয়ার্ড অনুসন্ধান করতে ব্যবহৃত হয়। হ্যাকাররা সাধারণত ডিকশনারি টুল ব্যবহার করে এই প্রক্রিয়াটি সহজলভ্য করে।

3. অ্যাট্যাক টুলস: হ্যাকাররা ব্রুটফোর্স অ্যাটাক করতে কম্পিউটার প্রোগ্রাম বা অ্যাটাক টুলস ব্যবহার করতে পারেন। এই অ্যাটাক টুলস হ্যাকারদেরকে স্বয়ংক্রিয়ভাবে ব্রুটফোর্স প্রক্রিয়াটি অত্যন্ত দ্রুত করে তুলে ধরতে সহায়তা করে।

এটি গুরুত্বপূর্ণ উল্লেখ যে ব্রুটফোর্স অ্যাটাক একটি অনৈতিক কার্যকর এবং অনুপযুক্ত। এটি অন্যান্য মানুষের অ্যাকাউন্ট বা সিস্টেমের নিরাপত্তার বিপরীতে করা হয়। অনুগ্রহ করে সর্বদা নৈতিক এবং আইনগত সীমাবদ্ধতা মেনে চলুন এবং কোনও অননুমোদিত হ্যাকিং প্রথা অনুসরণ করবেন না।

❖ অধ্যায় – ২.৩ : Keylogger?

Keylogger একটি সফটওয়্যার বা হার্ডওয়্যার টুল যা কীবোর্ডে টাইপ করা সমস্ত ইনপুট লগ করে রাখে। এটি একটি কারগর টুল যা ইনপুট লগ করে এবং তা হ্যাকারের কাছে পাঠায়। Keylogger ব্যবহার করে হ্যাকাররা ব্যবহারকারীদের টাইপ করা পাসওয়ার্ড, ব্যক্তিগত তথ্য, মেইল এবং অন্যান্য সংক্রান্ত তথ্যগুলি সংগ্রহ করতে পারে।

Keylogger তৈরি করা যেতে পারে বিভিন্ন পদ্ধতিতে, যেমন:

1. সফটওয়্যার ডেভেলপমেন্ট: কিছু প্রোগ্রামিং ভাষার সাহায্যে হ্যাকাররা একটি সফটওয়্যার তৈরি করতে পারেন যা কীবোর্ডে ইনপুট লগ করে রাখে। কম্পিউটারে ইনস্টল করা হয়ে থাকলে এই সফটওয়্যারটি হ্যাকারের কাছে ইনপুট সংগ্রহ করতে পারে।

2. হার্ডওয়্যার কীলগার: হ্যাকাররা হার্ডওয়্যার কীলগার ব্যবহার করে কীবোর্ডে ইনপুট লগ করতে পারেন। এটি কীবোর্ড সংযোগ করার সময় সংযোগপ্রদান করে এবং ইনপুট লগ করে এটি হ্যাকারের কাছে পাঠায়।

Keylogger হ্যাকিং হল কোনও ব্যবহারকারীর কীবোর্ড ইনপুট লগ করে সংগ্রহ করা এবং এই তথ্যগুলি হ্যাকারের কাছে পাঠানোর পদ্ধতি। Keylogger হ্যাকিং ব্যবহারকারীদের ব্যক্তিগত তথ্য, ব্যাংক একাউন্টের তথ্য, সামাজিক নেটওয়ার্ক একাউন্ট, মেইল পাসওয়ার্ড ইত্যাদি সংগ্রহ করতে পারে।

আবারও বলছি যে কিংবা কোনও হ্যাকিং প্রক্রিয়া অনুসরণ করা সম্পর্কে নৈতিক এবং আইনগত সীমাবদ্ধতা মেনে চলুন। হ্যাকিং প্রয়োজনীয় সাক্ষরতা ও অনুমতি ছাড়াই কোনও সিস্টেম বা সংস্থার নিরাপত্তার বিপরীতে ঘাচাচ্ছে এবং বিধিবদ্ধতার লঙ্ঘন করতে হয় না।

❖ অধ্যায় – ২.৪ : মোবাইল আপ্লিকেশন হ্যাক?

মোবাইল আপ্লিকেশন হ্যাক করা হল মোবাইল অ্যাপস এর নিরাপত্তার সুরক্ষা প্রতিরোধক প্রতিষ্ঠানকে পালন করতে হয়। হ্যাকাররা মোবাইল অ্যাপস এর সুরক্ষায় খোঁজ চলার অনুমতি পান এবং সেই অক্ষমতাকে অধিকার করে তাদের প্রয়োজনমত ক্রিয়াকলাপ চালাতে পারে।

মোবাইল আপ্লিকেশন হ্যাকিং এর কিছু উদাহরণ হতে পারে:
- অ্যাপস মধ্যে দুর্নীতি প্রবেশ করে ব্যবহারকারীর ব্যক্তিগত তথ্য সংগ্রহ করা।
- অ্যাপসের কোড মধ্যে ত্রুটি খুঁজে বের করে তা অপব্যবহার করে অ্যাপসে ভূল বা খারাপ ক্রিয়াকলাপ চালানো।
- অ্যাপসের কোডে সুরক্ষার কোনও ত্রুটি থাকলে অ্যাপসে ভুল ক্রিয়াকলাপ চালাতে পারে।

মোবাইল আপ্লিকেশন হ্যাকিং অনুসারক সংশ্লিষ্ট আইনগুলির লঙ্ঘন এবং ব্যবহারকারীদের নিরাপত্তার বিপরীতে ঘাচাচ্ছে যা নিষিদ্ধ এবং নিন্দিত। আপনাকে সুপারিশ করা হচ্ছে সুরক্ষার দিকে সচেষ্ট থাকতে এবং অননুমোদিত হ্যাকিং প্রথার প্রতিরোধ নিশ্চিত করতে।

❖ অধ্যায় – ২.৫ : LFI ওয়েব সাইট হ্যাকিং কি ?

LFI হলো Local File Inclusion (লোকাল ফাইল ইনক্লুশন) হতে পারে। এটি একটি হ্যাকিং পদ্ধতি যা একটি ওয়েব সাইটের কোডে লোকাল কম্পিউটারে স্থানান্তরিত করা হয়ে থাকা ফাইলগুলির সংযোগ ব্যবহার করে ওয়েব সাইটে অনুমতি প্রাপ্ত করতে ব্যবহার করা হয়।

LFI হ্যাকিং, হ্যাকার সাধারণতঃ ওয়েব সাইটে বিশেষভাবে তৈরি করা প্যারামিটার ব্যবহার করে কোনো ফাইলের নাম প্রদান করে। ফাইল নামের পরিবর্তে হ্যাকার লোকাল মেশিনে অন্য কোনো ফাইলের ঠিকানা সরবরাহ করতে পারে। যদি ওয়েব সাইট সঠিক নিরাপত্তা প্রদান না করে ফাইল নির্দেশ পরিবর্তন করলে, হ্যাকার লোকাল মেশিনের ফাইলের সাথে সংযুক্ত হতে পারে এবং এই সংযোগটি ব্যবহার করে অন্যান্য ক্ষেত্রে নিরাপত্তা উল্লঙ্ঘন করতে পারে।

একটি উদাহরণ হলো যদি ওয়েব সাইটের URL এ নিম্নরূপ প্যারামিটার উপস্থিত থাকে:

```
http://www.example.com/page.php?file=about.html
```

হ্যাকার যদি প্যারামিটারটি পরিবর্তন করে নিম্নরূপ হিসাবে সংযুক্ত করে:

```
http://www.example.com/page.php?file=/etc/passwd
```

তাহলে ওয়েব সাইটটি লোকাল মেশিনে অন্যান্য কোনো ফাইলের ঠিকানা পাঠাতে ব্যবহৃত হবে এবং হ্যাকার লোকাল মেশিনের `/etc/passwd` ফাইলের তথ্য অর্জন করতে পারে।

একটি প্রশাসনিক ভূমিকা পরিবর্তন করার মাধ্যমে, হ্যাকার লোকাল মেশিনের ক্ষেত্রে ভূমিকা বদলে দিতে পারে এবং লোকাল মেশিনে রাখা কোনো গোপন ফাইল অ্যাক্সেস করতে পারে।

LFI হ্যাকিংে অনেক সাধারণতঃ ওয়েব সাইটের নিরাপত্তা দুর্বলতা ব্যবহার করা হয় যা লোকাল ফাইলের সংযোগ প্রাপ্তির মাধ্যমে হ্যাকিং প্রাপ্ত করতে ব্যবহৃত হয়। সুরক্ষার ক্ষেত্রে প্রতিষ্ঠানসমূহকে অবগত হতে হবে এবং নিরাপত্তা বিষয়ক উন্নতি প্রয়োজন হবে যাতে LFI হ্যাকিং প্রতিরোধ করা যায়।

❖ অধ্যায় – ২.৬ : RFI ওয়েব সাইট হ্যাকিং কি ?

RFI এবং ওয়েব সাইট হ্যাকিং (RFI Web Site Hacking) হলো একটি অপ্রতিবেদনীয় হ্যাকিং পদ্ধতি যা একটি ওয়েব সাইটে অস্বীকৃতি উপস্থাপন বা কোড সংযোগ দ্বারা নির্দিষ্ট নির্দিষ্ট মধ্যস্থতা উপস্থাপন করতে ব্যবহার করে। এটি রিমোট ফাইল ইনক্লুশন

(Remote File Inclusion) হতে পারে বা আরেকটি ওয়েব সাইটের একটি বাংলা থেকে একটি নির্দিষ্ট ফাইলের কোড সংযোগের মাধ্যমে হতে পারে।

RFI হ্যাকিং একটি ক্রিমিনাল কার্যকর পদ্ধতি হওয়ার সাথে সাথে অনুমতি ছাড়াই একটি ওয়েব সাইটের মাধ্যমে প্রবেশের সুযোগ সৃষ্টি করে। এটি বিভিন্ন ধরণের আন্দোলন বা প্রদর্শনের সময় ওয়েবসাইটগুলিতে অপ্রতিবেদনীয় বার্তা বা ছবি পোস্ট করার উদ্দেশ্যে ব্যবহৃত হয়। এটি একটি ওয়েবসাইটে কোড সংযোগ বা উপস্থাপন করতে ব্যবহৃত হয় যেটি পরিবর্তন করতে একটি সম্ভাবনার হতে পারে বা আউটপুট নির্ভরতা বা অনির্ভরতা পরিবর্তন করতে পারে।

RFI হ্যাকিং আক্রান্ত ওয়েবসাইটের একটি কার্যকারিতা বা নিরাপত্তার স্তর অনুযায়ী তথ্য অধিগ্রহণ এবং কন্ট্রোল প্রাপ্ত করা যেতে পারে। এটি হ্যাকারদের সম্ভবত প্রাথমিক মাধ্যমে অন্য ধরণের হ্যাকিং পদ্ধতিগুলির জন্য অ্যাক্সেস সৃষ্টি করে তথ্য সংগ্রহ করার জন্য সহজলভ্য পথ প্রদান করে।

❖ অধ্যায় – ২.৭ : XXS ওয়েব সাইট হ্যাকিং কি ?

XXS ওয়েব সাইট হ্যাকিং হলো Cross-Site Scripting (ক্রস-সাইট স্ক্রিপ্টিং) হতে পারে। এটি একটি অপ্রতিবেদনীয় হ্যাকিং পদ্ধতি যা ওয়েব সাইটের নিরাপত্তার ক্ষমতা দুর্বলতার মাধ্যমে অন্য ব্যবহারকারীদের সংক্ষিপ্ত জাভাস্ক্রিপ্ট কোড পরিবেশিত করে তাদের ব্রাউজারে পাঠানোর মাধ্যমে তথ্য সংগ্রহ করার জন্য ব্যবহৃত হয়।

XXS হ্যাকিং একজন হ্যাকার অপ্রতিবেদনীয়ভাবে জাভাস্ক্রিপ্ট কোড অংশ সাংযোগিক করে একটি ওয়েব সাইটের পাতা বা অন্য ব্যবহারকারীর সাথে সংযুক্ত করে তথ্য সংগ্রহ করতে পারে। এটি ব্যবহারকারীদের ব্রাউজারের মধ্যে চালিত হয় এবং মালিকানাধীন সাইটের সাথে সংযুক্ত হয়ে থাকা ওয়েব সাইটের কন্টেক্সট এবং সাধারণতঃ ব্যবহারকারীর ব্রাউজারে স্ক্রিপ্ট এক্সিকিউশন সৃষ্টি করতে পারে।

XXS হ্যাকিংর পরিণামে হ্যাকার প্রধানতঃ ব্যবহারকারীর ব্রাউজারের মধ্যমে অপ্রতিবেদনীভাবে কোনো কার্যকর জাভাস্ক্রিপ্ট কোড সংযোগ করতে পারে এবং সংগ্রহিত তথ্য সংগ্রহ করতে পারে। এর মাধ্যমে হ্যাকার সাধারণতঃ ব্যবহারকারীর গোপন তথ্য (যেমন ব্যবহারকারীর পাসওয়ার্ড, অ্যাকাউন্ট তথ্য, কুকিজ) সংগ্রহ করতে পারে এবং এগুলি অন্য সাইটে অনুপ্রবেশ করতে ব্যবহার করতে পারে।

একটি উদাহরণ হলো যদি একটি ওয়েব সাইটে সংক্ষিপ্ত জাভাস্ক্রিপ্ট কোড সংযোগিত হয়, তাহলে হ্যাকার একটি নিরাপদ ওয়েবসাইটে একটি লিংক তৈরি করতে পারে যাতে যখন কেউ সেই লিংকে ক্লিক করে, সেই কোডটি সংগ্রহ করা হয়। এভাবে হ্যাকার ব্যবহারকারীর ব্রাউজারের মধ্যমে তথ্য প্রাপ্ত করতে পারে এবং আরও

অনেক কার্যকর হ্যাকিং পদ্ধতির জন্য সংগঠিত হতে পারে।

একে শুধুমাত্র সাধারণতঃ প্রদর্শিত করার উদাহরণ হিসাবে ব্যবহার করা হয়েছে। একটি সতর্কতা পরিমাপ হলো যেখানে অপ্রতিবেদনীয় কোড দূর্বলতা সংগত সাইটে নিরাপত্তা নিশ্চিত করার জন্য সামগ্রিক নিরাপত্তা সংক্রান্ত পরিষ্কার পর্যবেক্ষণ ও উন্নতি প্রয়োজন।

❖ অধ্যায় – ২.৮ : Ddos অ্যাটাক কি? এবং কিভাবে হয়?

DDoS অ্যাটাক (Distributed Denial of Service) হলো একটি হুমকি পরিস্থিতি, যা ওয়েবসাইট, অনলাইন সেবা বা নেটওয়ার্কের বিপদজনক পরিস্থিতি সৃষ্টি করে। এটি একটি অপরিচিত সংখ্যক কম্পিউটারের নেটওয়ার্ক সমন্বয় ব্যবহার করে হয়, যাতে সময় সীমানা এবং সংস্থান সীমানা ছাড়িয়ে যায়। একটি DDoS অ্যাটাক করার ফলে লক্ষ্যমূলক ওয়েবসাইট বা সার্ভারের জন্য সময়সীমানা ও উপলব্ধিতে সংকট সৃষ্টি হয়।

একটি DDoS অ্যাটাক কিভাবে কার্যকরী হয় তা নিম্নরূপঃ

1. হ্যাকার প্রায়শই বিভিন্ন জনসাধারণের কম্পিউটারে ম্যালওয়্যার অথবা বটনেট (botnet) নামে পর্যায়ক্রমে সংগ্রহ করে যা রাখা থাকে। এই কম্পিউটার সংগ্রহশ্রেণিতে সংক্রান্তভাবে কম্পিউটারের মালিকের অজানা থাকে।

2. হ্যাকার বটনেটের সাহায্যে একটি স্বতঃস্ফূর্ত নেটওয়ার্ক তৈরি করে যায়। এই বটনেটের সদস্য কম্পিউটার যদি কেবলমাত্র নির্দিষ্ট ধারণায় কাজ করে তবে তাকে "জীববিদ্যুতের ব্যবহারকারী" (zombie) বা "জীব" (bot) বলা হয়।

3. হ্যাকার বটনেট ব্যবহার করে একটি অবজেক্টিভের উপর হামলা শুরু করে তাকে ব্যান্ডউইথ ব্যবহার করে জমা করে। বহুল পরিস্থিতিতে, পরিস্থিতির শীর্ষবর্তী সীমানা প্রাপ্ত হয়। সাধারণতঃ, হ্যাকার বটনেটের সদস্যদের ব্যান্ডউইথ সমন্বয় করা হয় যাতে হামলা শক্তির সৃষ্টি করা যায়।

4. হ্যাকার তার লক্ষ্যমূলক সাইটের প্রতি একাধিক ধরনের নেটওয়ার্ক পরিকল্পনা অনুসরণ করে যাতে তারা হ্যামলা করতে পারে। উদাহরণস্বরূপ, একটি স্থানীয় নেটওয়ার্কে থাকতে পারে একটি অ্যাটাক সূত্র, একটি একত্রিত সংযোগ ব্য

বহার করে হ্যামলা করতে পারে এবং ইন্টারনেটের সামরিক বাধা দিয়ে যাত্রা করতে পারে এবং অনলাইন সেবা বা সাইটের সাধারণ কার্যক্রমের সাথে যুক্ত নয়।

DDoS অ্যাটাক কে সাধারণতঃ ব্যবহার করা হয় এইভাবেঃ

1. হ্যাকার কম্পিউটার বা বটনেটের সদস্য কেবলমাত্র একটি নির্দিষ্ট কম্পিউটারে বার্তা প্রেরণ করে হামলা শুরু করে।

2. হামলার বার্তাগুলি সম্ভবতঃ প্রতি সেকেন্ডে হয়ে থাকে এবং বিশেষ মেমোরি কার্যক্রম নিয়ন্ত্রণ বা স্থানীয় পাঠ্য ব্যান্ডউইথ উপলব্ধি করতে পারে।

3. লক্ষ্যমূলক ওয়েবসাইটে প্রায়শই বার্তাগুলি অত্যধিক পরিমাণে উপস্থিত থাকে এবং এটির ব্যান্ডউইথ সীমানা পার করে যায়। এটি কারণে লক্ষ্যমূলক ওয়েবসাইট বা সার্ভার নিষ্ক্রিয় হয়ে যায় এবং ব্যবহারকারীদের উপলব্ধিতে সমস্যা সৃষ্টি হয়।

DDoS হ্যাকিং প্রতিরোধের ক্ষেত্রে প্রাথমিক প্রতিরোধ ব্যবস্থা যেমন ব্যান্ডউইথ মান নিয়ন্ত্রণ, সার্ভারের সঠিক কনফিগারেশন এবং সিকিউরিটি মানদণ্ড পালন এসব উপযুক্ত কর্মসূচি গ্রহণ করা। এছাড়াও, ট্রাফিক মনিটরিং, ইনট্রাস্ট প্রিভেনশন সিস্টেম (IPS), ডস মিটিগেশন সার্ভিস, ক্লাউড ফায়ারওয়াল এবং অন্যান্য সুরক্ষা প্রয়োজনীয় সরঞ্জামসমূহ ব্যবহার করা যেতে পারে।

❖ অধ্যায় – ২.৯ : Dos অ্যাটাক কি? এবং কিভাবে হয়?

DoS (Denial of Service) অ্যাটাক হলো একটি হুমকি পরিস্থিতি, যা ওয়েবসাইট, সার্ভার বা নেটওয়ার্কের সেবা সংক্ষিপ্ত করে দেয়। এটি হ্যাকারের দ্বারা সাধারণতঃ ওয়েবসাইটের ব্যান্ডউইথ বা সার্ভারের সময়সীমানা উপলব্ধি করে তুলে ধরে সাধারণ ব্যবহারকারীদের ওয়েবসাইটে অ্যাক্সেস করা দুষ্কর বা সম্পূর্ণ বন্ধ করে দেয়।

DoS অ্যাটাক একটি সহজ পদ্ধতিতে হয় যাতে হ্যাকার একটি বা একাধিক কম্পিউটার ব্যবহার করে সৃষ্টি করে। এই কম্পিউটারগুলির জন্য হ্যাকার ম্যালওয়্যার বা টুলস ব্যবহার করে হ্যাকিং কার্যক্রম সহজলভ্য করে থাকে। হ্যাকার এই কম্পিউটারগুলির সাহায্যে টার্গেট সার্ভারে মারাত্মক মাত্রায় ডেটা প্রেরণ করে তার সময়সীমানা উপলব্ধি করে ধরে তুলে দেয়।

DoS অ্যাটাকের কিছু উদাহরণ নিম্নিখিতঃ

1. সার্ভারের বান্ডউইথ অতিক্রান্ত করে তাড়াতাড়ি অনেক অনুরোধ প্রেরণ করে তুলে দেয়।

2. সার্ভারের প্রসেসরের মাধ্যমে সময়সীমানা পরিবর্তন করে অতিক্রান্ত অনুরোধ প্রেরণ করে তুলে দেয়।

3. নেটওয়ার্কের সাথে যুক্ত কিছু আইপি প্যাকেট প্রেরণ করে তুলে দেয়, যা সিস্টেমের সামঞ্জস্যকে খুব বেশি পরিশ্রম করে দেয়।

এগুলি মাত্র কয়েকটি উদাহরণ, তবে DoS অ্যাটাকের আরও অনেক রকম হতে পারে যা হ্যাকার সিস্টেমে বা সার্ভারে অতিক্রান্ত অনুরোধ প্রেরণ করে সাধারণ ব্যবহারকারীদের সেবা সংক্ষিপ্ত করে দেয়।

❖ অধ্যায় - ২.১০ : SQL Injection ওয়েব সাইট হ্যাকিং

SQL Injection হলো একটি প্রকার ওয়েব আক্রমণ, যেখানে হ্যাকার অনলাইন এপ্লিকেশনের ডাটাবেসের SQL কোয়েরির মাধ্যমে অপ্রমাণিত বা মালিন ডেটা প্রদান করে অনুমানিত পরিবর্তন সাধারণতঃ করে। এর ফলে হ্যাকার বিভিন্ন ধরনের ক্ষতি করতে পারে, যেমন ডেটাবেসে তথ্যের পরিবর্তন, তথ্য প্রদান অসমর্থন, এক্সেস নিষ্ক্রিয় করা ইত্যাদি।

SQL Injection হ্যাকিং একটি কমন পদ্ধতি, যেখানে হ্যাকার বার্তা বা ইনপুট প্যারামিটারে একটি SQL কোয়েরির অসুবিধাজনক কোড অ্যাড করে। এর মাধ্যমে হ্যাকার অদৃশ্যভাবে একটি সহজলভ্য কোড বা বার্তা দিয়ে ডাটাবেস সার্ভারে প্রবেশ করে তারপর ডাটাবেসে কোন কিছু করে তুলে দেয়।

এটি অন্যতম সাধারণতঃ এইভাবে ঘটেঃ

1. হ্যাকার ওয়েবসাইটে প্রবেশ করে ইনপুট ফর্মের মাধ্যমে একটি SQL কোয়েরি প্রেরণ করতে পারে।

2. হ্যাকার মালিন বা ধ্বংসাত্মক SQL কোড ইনজেক্ট করতে পারে ইনপুট ফর্মের প্যারামিটারে।

3. ওয়েব অ্যাপ্লিকেশন সার্ভার হ্যাকারের ইনপুট অনুমতি দেয় এবং তারপর ক্লায়েন্ট দ্বারা প্রেরণ করা SQL কোয়েরি এক্সিকিউট করে দেয়।

এর মাধ্যমে হ্যাকার ডাটাবেসের সামগ্রিক নিরাপত্তা উল্লঙ্ঘন করতে পারে এবং গোপন তথ্যের অধিকার অর্জন করতে পারে।

❖ অধ্যায় - ২.১১ : SQL Injection ওয়েব সাইট হ্যাকিং কিভাবে করে এবং উদাহরন ?

SQL Injection হ্যাকিং একটি প্রধান পদ্ধতি হিসাবে ব্যবহার করা হয় যখন ওয়েব আপ্লিকেশনের ইনপুট ফর্মের প্যারামিটারে সমস্যাজনক কোড ইনজেক্ট করা হয়। এটির মাধ্যমে হ্যাকার অনলাইন এপ্লিকেশনের ডাটাবেসের সাথে সংযোগ স্থাপন করে এবং অনধিকারগ্রস্ত কাজ করতে পারে।

এটি যেভাবে কাজ করতে পারে সেটি ব্যাখ্যা করার জন্য একটি উদাহরণ দেখানো হলোঃ

ধরুন আপনার একটি ওয়েব সাইট রয়েছে যেখানে ইউজারকে লগইন করতে হয়। লগইন ফর্মে আপনার ইউজারনেম এবং পাসওয়ার্ড প্রদান করতে হয়। যখন ইউজার তথ্যগুলি সাবমিট করে তখন ওয়েব আপ্লিকেশনটি ব্যবহারকারীর ইনপুট দ্বারা সানিটাইজ না করে সরাসরি SQL কোয়েরির একটি স্ট্রিং তৈরি করে এবং সেটি ডাটাবেসের সাথে এক্সিকিউট করে।

একটি সাধারণ উদাহরণ দেখানো যাকঃ

লগইন ফর্মে ইউজারনেম হলো "admin" এবং পাসওয়ার্ড হলো "pass123". এখন যখন আপনি ইউজারনেম এবং পাসওয়ার্ড সাবমিট করেন, সানিটাইজেশন না করে ওয়েব আপ্লিকেশনটি একটি SQL কোয়েরি তৈরি করবে যেটি মতামত এবং সামগ্রিক কোয়েরি এক্সিকিউশন করে তারপর লগইন করবে।

যেমনঃ

```
SELECT * FROM users WHERE username = 'admin' AND password = 'pass123'
```

এখন যদি হ্যাকার ইনপুট ফর্মে ইনপুট হিসাবে নিম্নলিখিত কোড ইনজেক্ট করে তবে সে মতামতে আগমন করতে পারবেঃ

```
' OR '1'='1
```

এর ফলে তৈরি হয়ে যাবে নিম্নলিখিত কোয়েরিঃ

SELECT * FROM users WHERE username = '' OR '1'='1' AND password = ''

যেখানে '1'='1' শর্তটি সত্য হয়ে যাবে সবসময় এবং লগইন ক্রিয়াকলাপটি সম্পূর্ণ ব্যাপক হয়ে যাবে, এবং হ্যাকার লগইন করতে পারবে অপরিচিত ব্যবহারকারীর একটি অ্যাকাউন্টে।

এভাবে SQL Injection হ্যাকিং পদ্ধতি ব্যবহার করে হ্যাকাররা ডাটাবেসের সাথে সংযোগ স্থাপন করে অপ্রমাণিত বা মালিন ডেটা প্রদান করতে পারে, তথ্য পরিবর্ধন করতে পারে, তথ্য প্রদানে সমস্যা সৃষ্টি করতে পারে এবং অন্যান্য ক্ষতিসাধন করতে পারে।

ইউনিট - ০৩ : সোশ্যাল মিডিয়া হ্যাকিং

❖ অধ্যায় - ৩.১ : Facebook Hacking

ফেসবুক হ্যাকিং একটি অপ্রতিকূল কাজ এবং এটি অনৈতিক এবং গৈরকানুনের কার্য। ফেসবুক একটি প্রয়োজনীয় সুরক্ষার সাথে প্রতিপক্ষ এর ব্যবহারকারীদের তথ্য রক্ষা করার জন্য বিভিন্ন নিরাপত্তা মেয়াদকে সংশোধন করেছে। ফেসবুক হ্যাকিং এর কিছু সাধারণ পদ্ধতির উদাহরণ নিম্নলিখিতঃ

1. ফিশিং: ফিশিং হল প্রতারণা পদ্ধতি যার মাধ্যমে হ্যাকাররা প্রতারণা বা জালিয়াতি ওয়েবসাইটের মাধ্যমে ব্যবহারকারীদের ফেসবুক একাউন্টের তথ্য চুক্তি প্রদান করতে চেষ্টা করে। সাধারণত এটি মেইল বা মেসেঞ্জারে আসা একটি জালিয়াতি মেসেজের মাধ্যমে হয়। ব্যবহারকারীর তথ্য প্রদানের জন্য এই মেসেজ আকর্ষণীয় হয়ে থাকে যা অনুমানিত ফেসবুক সাইটের প্রচেষ্টা হিসাবে দেখা যায়।

2. ব্রুটফোর্স অ্যাটাক: এটি হ্যাকাররা একাউন্টের পাসওয়ার্ড অনুসন্ধানের জন্য বিভিন্ন কম্বিনেশনে পাসওয়ার্ড প্রদান করে দেখে একাউন্টে লগ ইন করার চেষ্টা করে। হ্যাকাররা সাধারণত ব্রুটফোর্স অ্যাটাক টুল ব্যবহার করে এই প্রক্রিয়াটি সহজলভ্য করে।

3. সোশ্যাল ইঞ্জিনিয়ারিং: এটি মানুষের মাধ্যমে হ্যাকাররা ব্যবহারকারীদের ধারণকে মার্জনীয় করার চেষ্টা করে। তারা মানুষের সামরিক অংশের জন্য বিভিন্ন প্রকার খেলাধুলা ব্যবহার করে এবং ব্যবহারকারীকে ধারণ দেওয়ার জন্য প্রাণান্তিক মতামত সৃষ্টি করে।

উল্লেখ্য যে ফেসবুক হ্যাকিং অবৈধ এবং প্রতিবন্ধী কর্ম। আপনাকে ফেসবুক একাউন্টের নিরাপত্তা বৃদ্ধি করার জন্য নির্দিষ্ট সুরক্ষা পদ্ধতি পরামর্শ দেয়া হয়। আপনি নিজের অ্যাকাউন্টের সুরক্ষা সেটিংস পর্যালোচনা করতে পারেন এবং সক্ষম অ্যাপস ব্যবহার করে যা আপনাকে সুরক্ষিত রাখবে। যদি আপনি কোনও সন্দেহভাজন কার্যকর হ্যাকিং অভিযান দেখেন বা অভিযোগ করতে চান, তাহলে আপনাকে সরাসরি ফেসবুকে জানাতে হবে।

❖ অধ্যায় - ৩.২ : Instagram Hacking

Instagram হ্যাকিং হল কোনও ব্যবহারকারীর Instagram অ্যাকাউন্টে অনধিকৃত প্রবেশ করে সেই অ্যাকাউন্টের নিয়ন্ত্রণ অর্জন করা। হ্যাকাররা বিভিন্ন পদ্ধতিতে Instagram অ্যাকাউন্ট অধিগ্রহণ করতে পারেন।

Instagram হ্যাকিংের কিছু উদাহরণ হতে পারে:

1. পাসওয়ার্ড প্রাপ্তি: হ্যাকাররা ব্যবহারকারীর পাসওয়ার্ড অধিগ্রহণ করার জন্য পাসওয়ার্ড ক্র্যাকিং টুল ব্যবহার করতে পারেন। যদি ব্যবহারকারীর পাসওয়ার্ড শক্তিশালী না হয় অথবা কোনও প্রশ্নোত্তর ভূলের মাধ্যমে হ্যাকাররা পাসওয়ার্ড অধিগ্রহণ করতে পারেন।

2. ফিশিং: হ্যাকাররা ফিশিং প্রক্রিয়া ব্যবহার করে ব্যবহারকারীদের মিথ্যা ওয়েবসাইটের মাধ্যমে পাসওয়ার্ড অধিগ্রহণ করতে পারেন। অন্যান্য ব্যবহারকারীদের মতো দেখতে হয় কিন্তু প্রদত্ত তথ্যগুলি হ্যাকাররাই পায়।

3. বুঝে নিলে অনধিকৃত অ্যাকাউন্ট প্রবেশ: হ্যাকাররা বিভিন্ন পদ্ধতিতে অনধিকৃত অ্যাকাউন্ট প্রবেশ করতে পারেন, যেমন সিকিউরিটি নির্দেশিকা ভুলে গেলে বা প্রদত্ত সেবার মাধ্যমে অ্যাকাউন্ট পরিচালনা করা যায়।

4. কুকি হৈজাক: হ্যাকাররা ব্যবহারকারীর ব্রাউজারের কুকি অধিগ্রহণ করে সেই কুকিগুলির মাধ্যমে অ্যাকাউন্টে প্রবেশ করতে পারেন।

5. সোশ্যাল ইঞ্জিনিয়ারিং: হ্যাকাররা সোশ্যাল ইঞ্জিনিয়ারিং প্রয়োগ করে ব্যবহারকারীদের ভুল ক্লিক করানো বা খারাপ লিঙ্ক দিয়ে পাসওয়ার্ড অধিগ্রহণ করতে পারেন।

এইগুলি কিছু উদাহরণ, কিন্তু দয়া করে মনে রাখবেন যে এই প্রথার অপ্রতিষ্ঠিত হওয়া উচিত নয় এবং এটি সম্পূর্ণ গ্রাহক নিয়ন্ত্রণ প্রাপ্তির জন্য ব্যবহৃত হয়। Instagram অ্যাকাউন্ট সুরক্ষা প্রতিরোধ

গুলি প্রয়োগ করুন এবং সাইবার সুরক্ষা নিয়ে সচেষ্ট থাকুন।

❖ অধ্যায় – ৩.৩ : Gmail Hacking

Gmail হ্যাকিং হল কোনও ব্যবহারকারীর Gmail অ্যাকাউন্টে অনধিকৃত প্রবেশ করে সেই অ্যাকাউন্টের নিয়ন্ত্রণ অর্জন করা। হ্যাকাররা বিভিন্ন পদ্ধতিতে Gmail অ্যাকাউন্ট অধিগ্রহণ করতে পারেন।

Gmail হ্যাকিংর কিছু উদাহরণ হতে পারে:

1. পাসওয়ার্ড প্রাপ্তি: হ্যাকাররা ব্যবহারকারীর পাসওয়ার্ড অধিগ্রহণ করার জন্য পাসওয়ার্ড ক্র্যাকিং টুল ব্যবহার করতে পারেন। যদি ব্যবহারকারীর পাসওয়ার্ড শক্তিশালী না হয় অথবা কোনও প্রশ্নোত্তর ভূলের মাধ্যমে হ্যাকাররা পাসওয়ার্ড অধিগ্রহণ করতে পারেন।

2. ফিশিং: হ্যাকাররা ফিশিং প্রক্রিয়া ব্যবহার করে ব্যবহারকারীদের মিথ্যা ওয়েবসাইটের মাধ্যমে পাসওয়ার্ড অধিগ্রহণ করতে পারেন। অন্যান্য ব্যবহারকারীদের মতো দেখতে হয় কিন্তু প্রদত্ত তথ্যগুলি হ্যাকাররাই পায়।

3. কুকি হৈজাক: হ্যাকাররা কুকি অধিগ্রহণ করে ব্যবহারকারীর ব্রাউজারের মাধ্যমে Gmail অ্যাকাউন্টে প্রবেশ করতে পারেন। কুকি হ্যাজাকিং ব্যবহার করে হ্যাকাররা ব্যবহারকারীর লগইন সেশন, পাসওয়ার্ড ইত্যাদি পরবর্তীতে ব্যবহার করতে পারেন।

দয়া করে মনে রাখবেন যে এই প্রথার অপ্রতিষ্ঠিত হওয়া উচিত নয় এবং এটি কানাড়িয়ান সাইবার আইনের বিরুদ্ধে পরিচালিত হয়। গুরুত্বপূর্ণ বিষয় হল আপনার অ্যাকাউন্টের সুরক্ষা প্রতিরোধগুলি যথাযথভাবে পালন করা। আপনি নিজেই নিয়ন্ত্রণ রাখুন আপনার পাসওয়ার্ড এবং সাইবার সুরক্ষা সম্পর্কিত নির্দেশিকা মেনে চলুন।

❖ অধ্যায় – ৩.৪ : Camera কিভাবে হ্যাক হয়?

ক্যামেরা হ্যাকিং অপ্রতিষ্ঠিত এবং অবৈধ কর্ম। ক্যামেরা হ্যাকিং মাধ্যমে অন্য ব্যক্তির ক্যামেরা পরিচালনা করা হয় অনুপযুক্তভাবে বা অননুমোদিতভাবে। ক্যামেরা হ্যাকিং কঠিন এবং সংকটপূর্ণ প্রয়াস, এটি অন্যদের গোপন ক্যামেরা প্রবেশ করে তাদের ব্যক্তিগত জীবনের সম্পর্কে অপরাধীকে অপরাধটি চালাতে দেয় এবং ব্যবহারকারীর গোপন তথ্য চুরি করে।

বিশ্বাসযোগ্যভাবে ক্যামেরা হ্যাকিং থেকে বাচার প্রথম ধাপ হলো আপনার ডিভাইসগুলির সুরক্ষামূলক অপডেট সম্পন্ন করা। নিচে কিছু ক্যামেরা সুরক্ষা পরামর্শ দেওয়া হলো:

1. ডিভাইসে সুরক্ষামূলক পাসওয়ার্ড ব্যবহার করুন।
2. ডিভাইসের সিস্টেম এবং অ্যাপগুলি সর্বদা আপডেট রাখুন।
3. অপরিচলিত অ্যাপস ইনস্টল না করুন এবং শুধুমাত্র সেগুলি সম্পর্কে বিশ্বাস করা যাবে না।
4. সন্ধানপূর্বক এবং গোপনিযুক্ত কোনও ওয়েবসাইট অথবা ইমেলে ক্লিক করবেন না যা অপ্রতিষ্ঠিত এবং আশংকাজনক হতে পারে।
5. যখনই সম্ভব, ডিভাইসের সামান্য সময়ের জন্য ক্যামেরা নিষ্ক্রিয় করুন।
6. প্রয়োজনে অতিরিক্ত ক্যামেরা প্রাইভেসি কভার ব্যবহার করুন।
7. ডিভাইসের নেটওয়ার্ক সুরক্ষামূলক রাখার জন্য পাবলিক ওয়াইফাই সংযোগে ব্যবহারে সতর্ক থাকুন।

এছাড়াও, আপনার ক্যামেরা ব্যবহারের সময় সাবধানতা পালন করুন। সেন্সিটিভ অফিস বা ব্যক্তিগত জায়গায় ক্যামেরা ব্যবহারের সময় বিশ্বাসযোগ্যতা ও গোপনীয়তা নিশ্চিত করতে নিম্নলিখিত কয়েকটি পরামর্শ মেনে চলুন:

1. স্থানে ক্যামেরা ব্যবহার করার আগে লোকের সাথে আপনার প্রশংসা এবং স্বীকৃতি প্রাপ্ত করুন।
2. ক্যামেরা একটি পাসওয়ার্ড দিয়ে সুরক্ষিত করুন।
3. অন্যদের সাথে ক্যামেরা স্থাপনের পর সাবধানে পরীক্ষা করুন যাতে কোনও গোপন ক্যামেরা না থাকে।
4. ক্যামেরা নিয়ে কাজ শেষ হলে তাকে বিচ্ছিন্ন করুন বা পাসওয়ার্ড পরিবর্তন করুন।

এই সকল প্রদর্শিত সুরক্ষা পরামর্শগুলি মানসিক আরোগ্য ও গোপনীয়তা নিশ্চিত করতে সাহায্য করবে। যদি আপনি ক্যামেরা হ্যাকিংর সন্দেহ করেন বা অন্যান্য সাক্ষাৎকারের সাথে সমস্যা থাকে, তবে সরাসরি আইন প্রশাসন বা সাইবার সুরক্ষা প্রতিষ্ঠানে যোগাযোগ করুন।

❖ অধ্যায় – ৩.৫ : Location কিভাবে হ্যাক হয়?

সাধারণত কোনও ব্যক্তি বা হ্যাকার একটি ডিভাইসের অবৈধ অ্যাক্সেস ব্যবহার করে না হয়ে কোনও নিশ্চিত লোকেশন ডাটা হ্যাক করে না। তবে কিছু ক্ষেত্রে ক্র্যাকাররা সাধারণত নিম্নলিখিত পদক্ষেপ ব্যবহার করে লোকেশন হ্যাক করতে চেষ্টা করতে পারেন:

1. একটি ম্যালওয়্যার ইনস্টল করা: ক্র্যাকাররা ম্যালওয়্যার ব্যবহার করে নিশ্চিত ডিভাইসে সন্ধানপূর্বক লোকেশন ডাটা অ্যাক্সেস করতে পারেন। ম্যালওয়্যার ইনস্টল হওয়ার সময়, এটি নিজেকে ডিভাইসের কন্ট্রোল একটিভেট করে যাতে সে সেন্সর, এসএমএস, মাইক্রোফোন ইত্যাদির মাধ্যমে লোকেশন ডাটা সংগ্রহ করতে পারে।

2. ফিশিং: ফিশিং হ্যাকাররা মানুষদের গোপন তথ্য প্রাপ্ত করতে পারেন, যা পরবর্তীতে লোকেশন ডাটা প্রবেশ করার জন্য ব্যবহৃত হতে পারে। এটি সাধারণত একটি প্রতারণা অথবা সামাজিক ইঞ্জিনিয়ারিং প্রক্রিয়া হিসাবে ঘটতে পারে, যেমন মেসেজ বা ইমেইলের মাধ্যমে মানুষকে প্রতারণা করে নিজের লোকেশন ডাটা প্রবেশ করতে প্রবেশ করতে প্রবেশ করতে প্রবেশ করতে প্রবেশ করতে পারে।

3. সাইবার সিকিউরিটি বিপ্লব: সিস্টেমের জন্য সুরক্ষা নয়ে আনা অবৈধ মাধ্যম ব্যবহার করে ক্র্যাকাররা সাইবার সিকিউরিটি বিপ্লব তৈরি করতে পারেন যাতে লোকেশন ডাটা পরিবর্তন করতে পারেন বা প্রায়শই যাতে ডিভাইস লোকেশন ট্র্যাক করতে পারেন।

উপরে উল্লিখিত উদাহরণগুলি অন্যান্য অবৈধ অ্যাক্সেস পদক্ষেপ সহ লোকেশন হ্যাকিং সম্ভাবনার কিছু উদাহরণ মাত্র। এই প্রকার অপ্রতিবন্ধিত অ্যাক্সেস থেকে নিজের সুরক্ষা পরিস্কার রাখার জন্য সাইবার সুরক্ষা সুস্থির হোন এবং ডিভাইসে সক্রিয় সুরক্ষা বৈশিষ্ট্য ব্যবহার করুন। সাধারণত, সুরক্ষার পাসওয়ার্ড, আপডেট সময়মতো সফ্টওয়্যার ও অ্যাপস, মিলনসার্ভারের ব্যবহার এবং আপনার ব্যবহারিক অভিজ্ঞতা পর্যালোচনা করা ভাল মানসিকতা। আপনার ডিভাইস এবং অনলাইন অ্যাকাউন্টের জন্য সুরক্ষা প্রাথমিকভাবে মেনে চলুন।

❖ অধ্যায় – ৩.৬ : Wi-Fi Hacking

ওয়াইফাই হ্যাকিং হল অন্যদের ওয়াইফাই নেটওয়ার্কে অনধিকৃত প্রবেশ পেতে চেষ্টা করা। এটি অবসান্ত ওয়াইফাই সংযোগ পাওয়া বা সাইবার হামলা চালানোর জন্য ব্যবহৃত হতে পারে।

কিছু সাধারণ ওয়াইফাই হ্যাকিং পদ্ধতির উদাহরণ হল:

1. পাসওয়ার্ড অ্যাক্র্যাক: হ্যাকার যখন ওয়াইফাই সংযোগের জন্য পাসওয়ার্ড চায়, তখন তিনি বিভিন্ন পদ্ধতি ব্যবহার করে পাসওয়ার্ড অনুদেশ প্রদান করতে পারে। সেই সময় একজন হ্যাকার আসল পাসওয়ার্ড প্রাপ্ত করার চেষ্টা করতে পারে বা কোনও দূরবর্তী কম্পিউটার প্রোগ্রাম ব্যবহার করে পাসওয়ার্ডটি ক্র্যাক করতে পারে।

2. ম্যান-ইন-দি-মিডল অ্যাটাক (Man-in-the-Middle Attack): হ্যাকার একটি মধ্যম দ্বারা ওয়াইফাই সংযোগ ইন্টারসেপ্ট করতে পারে এবং বাধা দিয়ে সাধারণত কর্মক্ষমতা দিতে পারে। হ্যাকার সংযোগ স্থাপন করে অনুপ্রবেশ প্রদান করতে পারে এবং সংযোগের সামগ্রী চুক্তিভদ্রতা বা তথ্যগুলি আদান-প্রদান সংক্রান্ত হ্যাকারের কাছে পাঠাতে পারে।

3. ওয়াইফাই পাসওয়ার্ড ক্র্যাকিং: হ্যাকাররা কমপক্ষের পাসওয়ার্ডগুলি ক্র্যাক করতে পারে যা ওয়াইফাই সংযোগের জন্য ব্যবহৃত হয়। এটি আমাদেরকে অব্যবহৃত বা শক্তিশালী পাসওয়ার্ড ব্যবহার করা থেকে বাচানোর জন্য গুরুত্বপূর্ণ এবং কঠিন পাসওয়ার্ড ব্যবহার করার প্রয়োজনকে মনে রাখতে বাধ্য করে।

এটি গুরুত্বপূর্ণ উল্লেখ্য যে, ওয়াইফাই হ্যাকিং একটি গৈরকানুনের প্রক্রিয়া যা বেশিরভাগ দেশে বা অন্য দেশে সমবেত কানুন দ্বারা নিষিদ্ধ। এটি অন্যান্যের নিজস্ব নেটওয়ার্কে অনধিকৃত প্রবেশ পেতে চেষ্টা করলে কঠিনভাবে শাস্তি পাওয়া যায় এবং আইনগত দুস্থ ব্যবহারের মামলায় আসতে পারে। সবসময় আপনার নিজের ওয়াইফাই নেটওয়ার্কে সুরক্ষিততা বজায় রাখার জন্য বিশেষভাবে যত্ন নিতে হবে।

ওয়াইফাই হ্যাকিং করার নিয়ম?

ওয়াইফাই হ্যাকিং করা হল অন্যের ওয়াইফাই নেটওয়ার্কে অনধিকৃত প্রবেশ পেতে চেষ্টা করা। এর জন্য হ্যাকাররা বিভিন্ন পদ্ধতি ব্যবহার করে ওয়াইফাই নেটওয়ার্কের সুরক্ষা মেয়াদকে ছলানো চেষ্টা করে। কিছু প্রমুখ ওয়াইফাই হ্যাকিং পদ্ধতির উদাহরণ নিম্নলিখিতঃ

1. ওয়ার ড্রাইভিং (War Driving): হ্যাকাররা ওয়ার ড্রাইভিং ব্যবহার করে প্রায়শই গাড়ির মাধ্যমে শহরের সবগুলো এলাকায় চলাচল করে এবং উপস্থিত ওয়াইফাই নেটওয়ার্কগুলির তথ্য সংগ্রহ করে। এর জন্য তিনি ওয়ায় বা অন্যান্য ওয়ায় স্ক্যানিং পরিকল্পনা ব্যবহার করে সমস্ত নেটওয়ার্কের তথ্য সংগ্রহ করতে পারেন।

2. পাসওয়ার্ড অ্যাক্র্যাক: হ্যাকাররা সংযোগের জন্য প্রয়োজনীয় পাসওয়ার্ড চায়। তারা বিভিন্ন পদ্ধতি ব্যবহার করে পাসওয়ার্ড অনুদেশ প্রদান করতে পারে যেমন দূরবর্তী কম্পিউটার প্রোগ্রাম ব্যবহার করে পাসওয়ার্ড ক্র্যাক করা বা স্নিফিং পদ্ধতি ব্যবহার করে সংযোগের সামগ্রী আদান-প্রদান ধারণ করতে পারেন।

3. ম্যান-ইন-দি-মিডল অ্যাটাক (Man-in-the-Middle Attack): হ্যাকাররা মধ্যম দ্বারা ওয়াইফাই সংযোগ ইন্টারসেপ্ট করতে পারে এবং বাধা দিয়ে সাধারণ কম্পিউটার কমিউনিকেশনকে বিদ্যমান করাতে পারে। একটি মধ্যমের সাহায্যে তিনি মধ্যবর্তী হতে পারেন এবং সংযোগের সামগ্রী চুক্তিভদ্রতা বা তথ্য আদান-প্রদান সংক্রান্ত হ্যাকারের কাছে পাঠাতে পারেন।

উল্লেখ্য যে ওয়াইফাই হ্যাকিং একটি গৈরকানুনের প্রক্রিয়া। আপনাকে আপনার নিজস্ব ওয়াইফাই নেটওয়ার্ক সুরক্ষিত রাখার জন্য সঠিক সুরক্ষা প্রদান করা উচিত।

হার্ডওয়্যার এবং সফটওয়্যার আপডেট রাখা, শক্তিশালী পাসওয়ার্ড ব্যবহার করা, ক্রিপ্টোগ্রাফিক প্রোটোকল ব্যবহার করা, ওয়াইফাই এনক্রিপশন সক্ষম করা, নেটওয়ার্ক ফায়ারওয়াল ব্যবহার করা এবং নেটওয়ার্কের সীমাবদ্ধতা সেট করা এমন কিছু সুরক্ষা প্রথার অন্তর্ভুক্ত করা উচিত। সাথে সাথে নতুনদের জন্য উচ্চতর স্তরের সক্ষমতা সংগ্রহ করা উচিত।

ইউনিট – ০৪ : হ্যাকিং এর জন্য সেরা সফটওয়্যার

অধ্যায় – ৪.১ : Burp Suite

Burp Suite একটি প্রোফেশনাল ওয়েব অ্যাপ্লিকেশন টেস্টিং টুলসেট যা হ্যাকিং, সিকিউরিটি আক্রমণ টেস্টিং এবং প্রোটোকল আন্ডরস্ট্যান্ডিং জন্য ব্যবহৃত হয়। বাদামী প্রশিক্ষণ এবং বিস্তৃত ফিচার সেটের জন্য পরিচিত বার্প সুইট প্রফেশনাল পেনিট্রেশন টেস্টারদের মধ্যে খুবই জনপ্রিয়।

বার্প সুইট অনেকগুলি মডিউল বা কম্পোনেন্ট থাকে, সম্প্রতি প্রথমত দুইটি প্রধান মডিউল যা হলো Burp Proxy এবং Burp Scanner। Burp Proxy ব্যবহার করে আপনি ওয়েব অ্যাপ্লিকেশন ট্রাফিক ইন্টারসেপ্ট করতে পারেন, রিপ্লে করতে পারেন, বিভিন্ন মডিফিকেশন পরিচালনা করতে পারেন এবং ইন্টারসেপ্টেড রিকুয়েস্ট এবং রেসপন্স পরীক্ষা করতে পারেন। Burp Scanner হলো একটি অটোমেটেড সিকিউরিটি স্ক্যানার যা সিকিউরিটি বুদ্ধিমত্তা পরীক্ষা করে ওয়েব অ্যাপ্লিকেশনের জন্য সাম্প্রতিক বিপন্ন ক্ষমতা ও রিসোর্সের কোনো বিশেষ কমপ্রেশন খোঁজ করে।

Burp Suite একটি ব্যবহারযোগ্য গ্রাফিকাল ইউজার ইন্টারফেস সরবরাহ করে যা আমদানি করতে সহায়তা করে এবং পারফরমেন্স ও সিকিউরিটির ক্ষেত্রে সম্পূর্ণ নিয়ন্ত্রণ অনুমতি দেয়। আপনি দ্বারা আদেশ পাঠাতে পারেন এবং ব্যাটাচে স্ক্যান চালাতে পারেন।

সংক্ষেপে, Burp Suite একটি শক্তিশালী ওয়েব অ্যাপ্লিকেশন টেস্টিং টুলসেট যা আপনাকে ওয়েব অ্যাপ্লিকেশন সিকিউরিটি পরীক্ষা এবং অভিজ্ঞতা বৃদ্ধির জন্য সহায়তা করে। এটি পেনিট্রেশন টেস্টারদের একটি পছন্দের টুল হিসাবে পরিচিত

অধ্যায় – ৪.২ : Nmap

Nmap (Network Mapper) হলো একটি ওয়ার্ক স্ক্যানিং টুল যা প্রোটোকল পরিচালনা, সুরক্ষা বিশ্লেষণ এবং নেটওয়ার্ক ম্যাপিং করার জন্য ব্যবহৃত হয়। এটি একটি ওয়ার্ক স্ক্যানার যা একটি নেটওয়ার্কে কাছাকাছি থাকা হোস্টগুলির জন্য পুরোপুরি অকার্যকর পোর্ট এবং সার্ভিস স্ক্যান করে।

Nmap একটি কমান্ড লাইন টুল হিসাবে ব্যবহৃত হয়, তবে ইউজারদের সুবিধার্থে গ্রাফিকাল ইউজার ইন্টারফেস সহজতর ব্যবহার করা যায় যেখানে ইউজাররা নেটওয়ার্ক স্ক্যান করতে পারেন, পোর্ট স্ক্যান করতে পারেন, সার্ভিসের জন্য স্ক্যান করতে পারেন এবং অনেক অন্যান্য পরিবর্তনশীল পার্যাপ্ত নেটওয়ার্ক স্ক্যানিং কার্যক্রম পরিচালনা করতে পারেন।

Nmap একটি বিশেষজ্ঞতা সম্পন্ন টুল যা নেটওয়ার্ক সিকিউরিটি পেনিট্রেশন টেস্টিং এবং সিস্টেম এডমিনিস্ট্রেশনের জন্য ব্যবহৃত হয়। এর মাধ্যমে ব্যবহারকারীরা নেটওয়ার্কের সার্ভার, রাউটার, ফায়ারওয়াল এবং অন্যান্য নেটওয়ার্ক ডিভাইসের ক্ষেত্রে প্রোটোকল, পোর্ট এবং সার্ভিসের নিরাপত্তা আদম্য করে তুলতে পারেন। এর মাধ্যমে ব্যবহারকারীরা নেটওয়ার্কের অবস্থান অনুসারে হোস্টের উপস্থিতি, সার্ভিস পরিচালনা, ওয়ার্ম আপ এবং অন্যান্য নেটওয়ার্ক কার্যক্রম সম্পর্কে সংশ্লিষ্ট তথ্য পেতে পারেন।

❖ অধ্যায় - ৪.৩ : XAMPP

XAMPP হলো একটি ওয়েব সার্ভার এপ্লিকেশন স্ট্যাক যা ব্যবহারকারীদের স্থানীয় পরিবেশে ওয়েব অ্যাপ্লিকেশন উপায়ে উন্মুক্ত করে। এটি অসংখ্য কম্পোনেন্টস এবং সার্ভার সফটওয়্যার সংগ্রহ করে যা ওয়েব ডেভেলপমেন্ট ও টেস্টিং জন্য ব্যবহার করা যায়।

XAMPP এর নামকরণটি একটি এক্রোস্টিক পদের সমষ্টি হিসাবে ধারণ করা যায়। "X" এইখানে প্রতীকটির অর্থ হলো সংযুক্ত অর্থাৎ প্রাকৃতিকভাবে প্রোগ্রামগুলি সংযুক্ত করে সার্ভার সেটআপ করার ব্যবস্থা। "A" হলো এপাচি ওয়েব সার্ভার, "M" হলো মাইএসকিউএল ডাটাবেস, "P" হলো PHP স্ক্রিপ্টিং ভাষা এবং "P" হলো পার্ল প্রোগ্রামিং ভাষা বোর্ডটি প্রকাশ করে।

XAMPP প্যাকেজটির সাথে একটি ওয়েব সার্ভার সহ প্রায়শই ব্যবহৃত সার্ভার সফটওয়্যার সংযোজিত থাকে, যা অ্যাপাচি ওয়েব সার্ভার, মাইএসকিউএল ডাটাবেস সার্ভার, পিএইচপি স্ক্রিপ্টিং ভাষা এবং পার্ল প্রোগ্রামিং ভাষা সহ অন্যান্য উপকরণগুলি সহায়ক করে। এছাড়াও এটি সহজতর করে ইনস্টল এবং ব্যবহার করা যায় এবং উইন্ডোজ, লিনাক্স, ম্যাক এবং সোলারিস অপারেটিং সিস্টেমে ব্যবহার করা যায়। বিশেষত, ওয়েব ডেভেলপাররা এটি ব্যবহার করে লোকাল হোস্ট উইব সাইটগুলি তৈরি এবং টেস্ট করতে পারেন।

❖ অধ্যায় - ৪.৪ : Acunetix

Acunetix হলো একটি অটোমেটেড ওয়েব অ্যাপ্লিকেশন সিকিউরিটি স্ক্যানার যা ওয়েবসাইট সিকিউরিটির অপরিহার্য অংশ। এটি একটি কর্মশালা স্ক্যানার যা ওয়েব অ্যাপ্লিকেশনগুলির নিরাপত্তা পরীক্ষা করে সংক্রান্ত সিকিউরিটি রিস্কগুলি সনাক্ত করে।

Acunetix এর মাধ্যমে ব্যবহারকারীরা ওয়েব অ্যাপ্লিকেশনগুলির নিরাপত্তা পরীক্ষা করতে পারেন এবং সিকিউরিটি দুর্বলতাগুলি সনাক্ত করতে পারেন। এটি ওয়েব সাইটের ক্রস-সাইট স্ক্রিপ্টিং, সিকিউরিটি মিসকনফিগারেশন, SQL ইনজেকশন, লগিন সনাক্তকরণ, ক্রস-সাইট রিসোর্স ফর্জারি (CSRF), অনুমতি সংক্রান্ত বিশেষ সমস্যাগুলি ইত্যাদি সনাক্ত করতে সক্ষম।

Acunetix এর বৈশিষ্ট্যগুলির মধ্যে আছে অটোমেটেড স্ক্যান, সিকিউরিটি রিপোর্টিং এবং পুনরায় পরীক্ষার সুযোগ, জবরজবরায় স্ক্যান প্রসেস সম্পাদন, কম্প্লায়ান্স স্ক্যান, ওয়েবসাইট মনিটরিং এবং ইন্টিগ্রেশন সুবিধা। এটি ওয়েব অ্যাপ্লিকেশন সিকিউরিটি টিমদের, পেনেট্রেশন টেস্টারদের এবং ডেভেলপারদের জন্য একটি উপযুক্ত সিকিউরিটি টুল হিসাবে ব্যবহার করা হয়।

❖ অধ্যায় - ৪.৫ : Loic

Loic হলো Low Orbit Ion Cannon (LOIC) নামক একটি ডেস্ট্রাক্টিভ ডস (Distributed Denial of Service) টুল। এটি ইন্টারনেট সংযোগ অনুসারে বিভিন্ন কম্পিউটারের মাধ্যমে অধিক পরিমাণে ট্রাফিক উৎপন্ন করে একটি নির্দিষ্ট ওয়েবসাইট বা সার্ভারের উপর একটি ডস হামলা চালানোর জন্য ব্যবহার করা হয়।

LOIC এর উদ্দেশ্য হলো টারগেট ওয়েবসাইটে অতিসংখ্যে রিকোয়েস্ট পাঠানো এবং সার্ভার সংযোগের সীমার উপর দায়িত্ব প্রদান করা। এটি মাসকট কনসল ইউজার ইন্টারফেসের মাধ্যমে সহজেই ব্যবহার করা যায়। LOIC প্রয়োগে সংক্রান্ত কম্পিউটারের IP এড্রেস ও বন্দুক সংক্রান্ত সেটিংস প্রয়োজন হয়।

LOIC এর ব্যবহার একটি দণ্ডনীয় অপরাধ এবং নৈতিকতার বিরুদ্ধে। এটি অন্যান্য কম্পিউটারের সেবা দেয়া থেকে বিরত থাকুন এবং প্রশিক্ষিত একটি কম্পিউটার নেটওয়ার্ক সিকিউরিটি পেশাদারের নির্দেশাবলী অনুসরণ করুন।

ইউনিট – 05 : ভাইরাস

❖ অধ্যায় – ৫.১ : ভাইরাস সম্পর্কে বিস্তারিত ?

ভাইরাস হলো একটি ক্ষতিকর কম্পিউটার প্রোগ্রাম বা কোড, যা স্বাধীনভাবে প্রতিষ্ঠিত হয় এবং অন্যান্য প্রোগ্রামের উপর নথিপত্র সংযোগ করতে পারে। ভাইরাস একটি অস্থায়ী অবস্থায় রয়েছে এবং এটি স্বাধীনভাবে প্রপাগেট হয়ে যেতে পারে, তাই এটি অন্য প্রোগ্রামের কোড ও ডেটা বা সিস্টেমের কোনো অংশকে ক্ষতিকারক করতে পারে।

ভাইরাস কম্পিউটারের প্রধান কাজকে ভাংগ দেয় এবং ব্যবহারকারীর অপরাধ বা অনিয়মিত ক্রিয়াকলাপ পরিচালনা করতে পারে। ভাইরাস বিভিন্ন ধরণের হতে পারে যেমন ফাইল ভাইরাস, বুট সেক্টর ভাইরাস, মাইক্রোসফট ওয়ার্ম ইত্যাদি। এছাড়াও ভাইরাস বিভিন্ন উদ্দেশ্যে তৈরি করা হয়, যেমন তথ্য চুরি, ব্যবহারকারীদের নিজস্ব তথ্য চুরি, কম্পিউটার নিয়ন্ত্রণ ইত্যাদি।

ভাইরাসের মধ্যে অন্যতম একটি গুরুত্বপূর্ণ বৈশিষ্ট্য হলো স্বপ্নান্ত অনুষ্ঠানিক কোড থাকা। এই কোডের মাধ্যমে ভাইরাস নিজেকে স্থানান্তর করতে পারে এবং একটি সিস্টেমের প্রসারিত অংশ হিসাবে বৃদ্ধি পায়। ভাইরাস ব্যবহারকারীর অনুজ্ঞায় বা অন্য কোনো পরিবেশের অভাবে সক্রিয় হয় এবং স্থানান্তর করা হয়।

একটি ভাইরাসের মধ্যে আরও একটি গুরুত্বপূর্ণ বৈশিষ্ট্য হলো স্বপ্নযাত্রা ক্রিয়া। এটি অর্ধ-স্বপ্নের মতো কাজ করে এবং কম্পিউটারের সিস্টেম বা প্রোগ্রামে পরিবর্তন করতে সক্ষম হয়। ভাইরাস সক্রিয় হয়ে থাকলে এর পরিবর্তে পরিবর্তনশীল কোনো কার্য বা প্রদর্শন হতে পারে, যেমন তথ্য লিখতে, তথ্য মুছতে, কম্পিউটার নিয়ন্ত্রণ করতে এবং ইন্টারনেটে ডেটা প্রেরণ করতে পারে।

সাধারণত ভাইরাস প্রচালনা করতে একটি হোস্ট প্রোগ্রাম বা ফাইলের মধ্যে একটি গোপন উপাত্ত থাকে, যার মাধ্যমে এটি নিজেকে সক্রিয় করতে পারে। এই উপাত্ত অন্যকে নিরাপদে রাখা থেকে আপনার কম্পিউটারকে ভাইরাস থেকে সুরক্ষিত রাখার কারও দায়িত্ব নেই।

ভাইরাসের প্রধান উদ্দেশ্য হলো কম্পিউটারে ক্ষয়কর ক্রিয়া পরিচালনা করা, তথ্য চুরি করা এবং প্রদর্শন বা নিয়ন্ত্রণ নেয়া। কিছু ভাইরাস তৈরি করা হয় একটি ক্ষতিকর পরিচালক বা ব্যবহারকারীকে আরও ব্যাপক প্রাধান্য দেওয়ার জন্য, যেমন তথ্য নষ্ট করা, কম্পিউটার নিয়ন্ত্রণ করা ইত্যাদি। ভাইরাস সংক্রান্ত জরুরি বিষয়গুলি অন্য প্রোগ্রাম বা ফাইলে লেখা অপরিবর্তিত করতে পারে, ফাইলগুলির অস্তিত্ব নষ্ট করতে পারে, কম্পিউটারের কাজ নিষ্পত্তি করতে পারে এবং অন্যান্য ক্ষতিকারক ক্রিয়াকলাপ পরিচালনা করতে পারে।

ভাইরাসের জনপ্রিয় হওয়ার কারণে, প্রায় সকল কম্পিউটারে এন্টিভাইরাস সফটওয়্যার ব্যবহার করা হয়। এই সফটওয়্যার ভাইরাসগুলির চিহ্নাংকন করতে পারে এবং তাদের নিষ্পত্তি করার চেষ্টা করে। ভাইরাস থেকে সুরক্ষিত থাকার জন্য, নিরাপত্তা সংক্রান্ত উপদেশাবলী মেনে চলা উচিত, স্যাফটওয়্যার এবং অ্যাপডেটগুলি নিয়মিতভাবে আপডেট করা উচিত এবং অজানা উৎপাদনগুলি ডাউনলোড এবং ইনস্টল করার আগে ভাইরাস স্ক্যানার দ্বারা পরীক্ষা করা উচিত।

❖ অধ্যায় – ৫.২ : কম্পিউটারে ভাইরাস সম্পর্কে বিস্তারিত

কম্পিউটারে ভাইরাস হলো একটি ক্ষতিকর সফটওয়্যার প্রোগ্রাম যা ব্যবহারকারীর জ্ঞান ব্যতিক্রম বা অনুপযুক্ত কার্যক্রম পরিচালনা করে এবং কম্পিউটার সিস্টেমে ক্ষয়কর পরিবর্তন সৃষ্টি করে। এটি ধরনের একটি ম্যালওয়্যার (Malware) হিসাবে পরিচিত।

ভাইরাস একটি প্রোগ্রাম যা নিজেকে অন্য একটি সক্রিয় প্রোগ্রামের মধ্যে সংযোগ স্থাপন করতে পারে এবং নিজেকে নকসায় ছড়িয়ে তুলতে পারে। একটি ভাইরাস সংক্রান্ত গুরুত্বপূর্ণ বৈশিষ্ট্য হলো এটি অন্য ক্ষতিকর প্রোগ্রামগুলির মধ্যে প্রতিস্থাপন করতে পারে এবং নিজের নকসায় ছড়িয়ে তুলতে পারে নকসায় প্রদান করা ডেটা বা তথ্য সংগ্রহ করতে পারে। ভাইরাস কম্পিউটার সিস্টেমে অন্যান্য কম্পিউটার ফাইলগুলির পরিবর্তে নকসায় ফাইল সৃষ

ৃটি করতে পারে, কম্পিউটার সিস্টেমের কাজকর্ম বা নেটওয়ার্ক কানেকশনগুলির সাথে বিচ্ছিন্নতা সৃষ্টি করতে পারে এবং অন্য কম্পিউটার সিস্টেমগুলির ক্ষতিকারক হ্রাস প্রদান করতে পারে।

ভাইরাস বিস্তারিত করে তথ্য সংরক্ষণ করতে পারে, প্রদান করতে পারে অন্য সফটওয়্যারগুলির কাছে সংগ্রহিত তথ্য, কম্পিউটার ব্যবহারকারীর কাছে প্রদান করা সাধারণ তথ্য, ব্যবহারকারীর ইন্টারনেট গবেষণা ও ব্রাউজিং ইত্যাদি নকসায় করতে পারে। ভাইরাসের প্রধান উদ্দেশ্য হলো কম্পিউটার সিস্টেমে ক্ষয়কর পরিবর্তন সৃষ্টি করা এবং ব্যবহারকারীদের অব্যাহতি ও ব্যবহারকারী তথ্যের অপদার্থতা সৃষ্টি করা।

ভাইরাস প্রতিরোধের জন্য ব্যবহারকারীরা ভাইরাস স্ক্যানার, ফায়ারওয়াল, আন্টিভাইরাস সফটওয়্যার এবং সঠ

িক অনলাইন সুরক্ষা প্রথম ব্যবহার করে অপসারণ করতে পারেন। সংগ্রহিত তথ্যের ব্যাকআপ তৈরি করতে ও আপডেট ও সিকিউরিটি প্যাচগুলি সময় সাময়িক প্রদান করতে হয়। এছাড়াও সুরক্ষা সংক্রান্ত উপদেশ ও অভিযোগের মাধ্যমে ব্যবহারকারীরা ভাইরাস হ্যাকিং থেকে নিজেকে সুরক্ষিত রাখতে পারেন।

❖ অধ্যায় – ৫.৩ : মোবাইল ভাইরাস সম্পর্কে বিস্তারিত ?

মোবাইল ভাইরাস হলো একটি ক্ষতিকর সফটওয়্যার বা কোড, যা মোবাইল ডিভাইসে সংক্রমিত হয় এবং তথ্য চুরি, ক্র্যাশ করা বা অন্যান্য অপ্রয়োজনীয় ক্রিয়াকলাপ সম্পাদন করতে পারে। মোবাইল ভাইরাস বিভিন্ন উদ্দেশ্যে তৈরি করা হয়, যেমন ব্যক্তিগত তথ্য চুরি, ফিশিং আক্রমণ, ডিভাইসের নিয়ন্ত্রণ পরিচালনা, জালি অ্যাপস ইনস্টলেশন, ব্যক্তিগত তথ্য সংগ্রহ ইত্যাদি।

মোবাইল ভাইরাস প্রধানত অ্যাপস থেকে সংক্রমিত হয়। কিছু ক্ষতিকর অ্যাপস বা জালি অ্যাপস মোবাইলে ইনস্টল করলে তারা আপনার ডিভাইসে নিজেকে সক্রিয় করতে পারে এবং আপনার তথ্য সংগ্রহ করতে পারে। আরও কিছু ভাইরাস প্রকার নিউন্তনের জন্য সোশ্যাল মিডিয়া প্ল্যাটফর্ম, মেসেঞ্জার অ্যাপস, ইমেল আকাউন্ট ইত্যাদি ব্যবহার করা হয়।

মোবাইল ভাইরাস এলাকাভুক্ত হয় নিম্নলিখিত উদাহরণগুলি থেকে:

- জালি অ্যাপস: অন্যান্য অ্যাপসের নামে সাধারণত কিছু জালি অ্যাপস মোবাইল ডিভাইসে ইনস্টল করা হয়, যা অন্যান্য অ্যাপসের তথ্য চুরি করতে পারে।

- ফিশিং অ্যাটাক: প্রতারকরা আকারে মোবাইল ডিভাইসে ফেক অ্যাপস বা ফেক ওয়েবসাইট ব্যবহার করতে পারে, যা ব্যবহারকারীর ব্যক্তিগত তথ্য চুরি করতে পারে।

- ট্রোজান হর্স: ট্রোজান হর্স মোবাইল ডিভাইসে লুকিয়ে থাকতে পারে এবং ব্যক্তিগত তথ্য চুরি করতে পারে, অ্যাক্সেস নিয়ে ডিভাইসে কন্ট্রোল নেওয়া এবং আরও অন্যান্য ক্রিয়াকলাপ পরিচালনা করতে পারে।

মোবাইল ভাইরাস হ্যাকিং থেকে সুরক্ষিত থাকার জন্য, নিম্নলিখিত কিছু পরামর্শ মেনে চলা উচিত:

- যখনই সম্ভব, অফিশিয়াল সোর্স থেকে অ্যাপস ইনস্টল করুন এবং অন্যান্য অ্যাপস থেকে অজানা অ্যাপস ইনস্টল করা থেকে বিরত থাকুন।

- সিকিউর পাসওয়ার্ড ব্যবহার করুন এবং পাসওয়ার্ড পরিবর্তন করার জন্য নির্দিষ্ট সময়কাল পরিপূর্ণ করুন।

- মোবাইল অ্যান্টিভাইরাস সফটওয়্যার ইনস্টল করুন এবং নির্দিষ্ট সময়কালে ডিভাইস স্ক্যান করুন।

- উন্নত সংজ্ঞায়িত সংযোগ ব্যবহার করুন এবং অজানা ওয়াইফাই নেটওয়ার্কে সংযোগ থেকে বিরত থাকুন।

- অপডেট করা সম্পূর্ণ ওয়ান সময়ে আপনার মোবাইল অপারেটিং সিস্টেম এবং অ্যাপসগুলি রাখুন।

শেষ মনে রাখবেন, মোবাইল ভাইরাস থেকে সুরক্ষিত থাকতে সঠিক সংরক্ষণ, জনসাধারণ সুপারিশ প্রয়োজন এবং সঠিক সাইবার সুরক্ষা প্রথা মেনে চলা।

❖ অধ্যায় – ৫.৪ : Malware সম্পর্কে বিস্তারিত?

ম্যালওয়্যার হলো ক্যাটাগরিভিত্তিক সফটওয়্যারের একটি শক্তিশালী উপস স্থাপন যা ব্যবহারকারীর জ্ঞান অনুমতি ছাড়াই ব্যবহার করা হয়। ম্যালওয়্যার অনেক প্রকার হতে পারে যেমন ভাইরাস, ওয়ার্ম, ট্রোজান, রুটকিট ইত্যাদি। এই ম্যালওয়্যার অন্য কম্পিউটারের তথ্য অপরিবর্তিত করতে এবং কম্পিউটারে ক্ষতিকারক পরিবর্তন সাধারণত সাধারণ করে সেট করতে পারে।

ম্যালওয়্যার অধিকাংশই জানবে ব্যবহারকারীর জ্ঞান অনুমতি ছাড়াই সিস্টেমে প্রবেশ করার পথ বা উপায়। এটি যখন ক্ষতিকারক হয়, তখন এটি সংশ্লিষ্ট কম্পিউটার বা নেটওয়ার্কের সুরক্ষা সংশ্লিষ্ট সমস্যার সাথে ব্যক্তিগত তথ্য চুরি করতে পারে এবং ব্যবহারকারীর ব্যক্তিগত তথ্য প্রকাশ করতে পারে।

ক্যাটাগরিভিত্তিক ম্যালওয়্যার হতে পারে ব্যবহারকারীর সঙ্গে সংযোগ স্থাপন করে এবং প্রাথমিক অনুমতি ছাড়াই ব্যবহারকারীর গোপন তথ্য সংগ্রহ করতে পারে। অনেক ম্যালওয়্যার ব্যবহারকারীর ব্যক্তিগত তথ্য, যেমন ব্যবহারকারীর নাম, ইমেল ঠিকানা, ক্রেডিট কার্ড তথ্য ইত্যাদি চুরি করতে পারে।

❖ অধ্যায় – ৫.৫ : Spyware সম্পর্কে বিস্তারিত ?

স্পাইওয়্যার একটি অস্থায়ী বা গোপন কম্পিউটার সফটওয়্যার যা ব্যবহারকারীর জানবে না এবং ব্যবহারকারীর সম্মতিহীন অভিব্যক্তি করে ব্যবহারকারীর অবস্থান, ইন্টারনেট গবেষণা, টাইপ করা তথ্য, অ্যাকাউন্ট তথ্য, পাসওয়ার্ড ইত্যাদি আদান-প্রদান সংক্রান্ত ব্যক্তিগত তথ্য সংগ্রহ করতে পারে। স্পাইওয়্যার কম্পিউটারে স্থাপিত হয় স্টেলথিলি বা অপ্রত্যাশিতভাবে এবং ব্যবহারকারীর অবজেক্টিভদৃষ্টিতে অজানা অ্যাকশনগুলি পরিচালনা করতে পারে।

স্পাইওয়্যার বিশ্বস্ততা উপেক্ষা করে ব্যবহারকারীদের পরামর্শ করে যে সমস্ত সংস্থা বা প্রতিষ্ঠানগুলি সবসময় ব্যক্তিগত তথ্য সংরক্ষণ ও নিরাপত্তায় নিশ্চিত হয়। স্পাইওয়্যার একটি ব্যবহারকারীর অনুমতি ছাড়াই ইনস্টল হয়ে থাকতে পারে এবং এটি স্বয়ংক্রিয়ভাবে কার্যকর হয়ে থাকতে পারে অথবা সাদাসিধে উপযুক্ত লিঙ্ক বা সংযোগ মাধ্যমে ইনস্টল হয়ে যেতে পারে।

স্পাইওয়্যারের কিছু উদাহরণ হলো কিলট লগার, স্ক্রিনশট রেকর্ডার, কিলট ওয়েবক্যাম, কিলট মাইক্রোফোন ইত্যাদি। এই ধরনের সফটওয়্যার অনুকরণ করার সাথে সাথে ব্যবহারকারীর সংক্ষিপ্তস্থায়ী তথ্য গাড়ি নিয়ে চলে যায় যাতে পরবর্তীতে ব্যবহার করা যায়।

স্পাইওয়্যার থেকে সুরক্ষিত থাকতে ব্যবহারকারীরা একটি ভাইরাস স্ক্যানার ও সিকিউরিটি সফটওয়্যার ব্যবহার করতে পারেন, যারা সক্ষম হবে স্পাইওয়্যার কিছুই না হয়ে চলে আসায় এবং কম্পিউটারে প্রতিরোধ উপায় গ্রহণ করতে পারেন। এছাড়াও উচ্চ স্তরের সাইবার নিরাপত্তা প্রদান করতে সক্ষম সিকিউরিটি প্যাচ ও সিকিউরিটি আপগ্রেড ব্যবহার করা উচিত।

এছাড়াও একটি পাসওয়ার্ড ম্যানেজার ব্যবহার করা যাতে শক্তিশালী এবং ভিন্ন প্রকারের পাসওয়ার্ড ব্যবহার করা যায়। বাস্তবায়নে সঠিক সাইবার নিরাপত্তা অভিযান অনুসরণ করা উচিত যাতে নতুন এবং তথ্যবাহী প্রযুক্তির সাথে মিশে প্রাকৃতিক সাইবার নিরাপত্তা উপেক্ষা করা না যায়।

❖ অধ্যায় – ৫.৬ : Ransomware সম্পর্কে বিস্তারিত ?

র‍্যানসমওয়্যার (Ransomware) একটি সংকেত বা ম্যালওয়্যার প্রোগ্রাম, যা কম্পিউটার বা ডিজিটাল উপকরণের ডেটা এনক্রিপ্ট করে এবং ব্যবহারকারীর থেকে একটি প্রতিফলন হিসাবে ধনাদেশ বা বিশিষ্ট কী চাওয়া হয়। একবার কম্পিউটার বা সিস্টেম এনক্রিপ্ট করা হলে, একটি র‍্যানসম নোট বা সংকেত বার্তা প্রদর্শিত হয়, যেখানে আত্মসাত করার জন্য একটি পেশকারের থেকে টাকা অথবা ক্রিপ্টোকারেন্সি (যেমন বিটকয়েন) দাবি করা হয়। র‍্যানসমওয়্যার হ্যাকাররা সাধারণত পরিশোধের জন্য ক্রিপ্টোকারেন্সি ব্যবহার করে, যা ট্রানজেকশনের পরিপূর্ণতা এবং পরিস্থিতিতে অনুসারে নিয়ন্ত্রণযোগ্য হতে পারে।

র‍্যানসমওয়্যার হ্যাকিং সাধারণত কম্পিউটার বা ডিজিটাল সিস্টেমের উপর বিভিন্ন উপায়ে সন্ধান করে প্রবেশ করে। এটি একটি প্রমুখ মাধ্যম হলো ফিশিং ইমেইল, অস্থায়ী ওয়েবসাইট, অদ্যতিত সুরক্ষার দুর্বলতা, স্ক্রিপ্ট ভুল, জনগণের উপভোগযোগ্যতার উপর ভিত্তি করে ধরার মতো মার্গের মাধ্যমে ব্যবহারকারীকে আকর্ষণ দেয়। র‍্যানসমওয়্যার অথবা ম্যালওয়্যার প্রবেশ করার পরে, এটি সিস্টেমের ডেটা এনক্রিপ্ট করে এবং ব্যবহারকারীর প্রতিফলন প্রদর্শন করে।

র‍্যানসমওয়্যার হ্যাকিং সম্প্রতি একটি গুরুত্বপূর্ণ সাইবার অপরাধে পরিণত হয়েছে, এটি ব্যবহারকারীর ব্যক্তিগত ডেটা এবং ব্যবহারকারীর প্রাথমিকতা তথ্যগুলি দখল করতে পারে। এটি প্রতিষ্ঠানের কাছে তুলনামূলক নুষ্ঠানের কারণে পরিস্থিতিটি কিছুটা গুরুত্বপূর্ণ করে এবং প্রাথমিক দণ্ডনীয় অপরাধের বিষয়বস্তু হিসাবে বিবেচিত হয়। র‍্যানসমওয়্যার হ্যাকিং করে হ্যাকাররা প্রতিষ্ঠানকে টাকা প্রদানের জন্য দণ্ড চাওয়ার পাশাপাশি সাধারণ ব্যবহারকারীদের বিরক্তি ও কার্যকলাপের জন্যও উদ্দীপ্ত করতে পারে।

❖ অধ্যায় – ৫৭ ট্রোজান সম্পর্কে বিস্তারিত ?

ট্রোজান একটি ম্যালওয়্যার টাইপ যা অন্য কোনো জানার অজানা দ্বারা স্থাপিত হয়ে থাকে এবং সচরাচর একটি সাধারণ অ্যাপলিকেশন, ফাইল বা প্রোগ্রামে বদলে যায় যা ব্যবহারকারীর জ্ঞান ব্যতীত অবাস্তব কাজ সম্পাদন করতে পারে। ট্রোজান অধিকাংশই অন্য ম্যালওয়্যারের সাথে যুক্ত হয়ে থাকে যাতে তিনি ব্যবহারকারীর ডিভাইসে অনুপ্রাণিত দ্বারা নিয়ন্ত্রিত হতে পারেন এবং কিছু ক্রিয়াকলাপ পরিচালনা করতে পারেন।

ট্রোজান বানানো হয় বিভিন্ন উদ্দেশ্যে যেমন ব্যক্তিগত তথ্য চুরি, ডিভাইস নিয়ন্ত্রণ, ব্যবহারকারীর সম্মতি ছাড়াই কম্পিউটারে প্রবেশ ও প্রতারণা ইত্যাদির জন্য। ট্রোজান কম্পিউটারের সামগ্রিক সুরক্ষা সংক্রান্ত সমস্যার সৃষ্টি করতে পারে এবং ব্যবহারকারীদের গোপনীয় তথ্য সম্পর্কে গোপনীয়তা ঝাড়াতে পারে।

ট্রোজান সংক্রান্ত একটি গুরুত্বপূর্ণ বিশেষত্ব হলো সেটি আমদানি করার সময় সরাসরি ম্যালওয়্যার হিসাবে চিহ্নিত হয় না, বরং অপরিচিত স্রোত থেকে ডাউনলোড করা অ্যাপলিকেশন, সংলাপগুলি বা অন্যান্য ফাইলগুলির মধ্যে গোপন থাকতে পারে।

ট্রোজান থেকে সুরক্ষিত থাকতে নিম্নোক্ত কিছু কর্মপরিকল্পনা অনুসরণ করুন:

- এন্টিভাইরাস সফটওয়্যার এবং ম্যালওয়্যার রিমোভাল টুলস ব্যবহার করুন এবং নির্দিষ্ট সময়কালে আপডেট করুন।

- সন্দেহভাজনদের থেকে ম্যালিশাস সম্পর্কে সতর্ক থাকুন এবং অজানা অ্যাপস বা সুপারিশকৃত সোর্স থেকে কোনো সংলাপ ইনস্টল না করে পর্যালোচনা করুন।

- উপযুক্ত মোবাইল সুরক্ষা অ্যাপস ইনস্টল করুন এবং নির্দিষ্ট সেটিং করে অ্যাপ ইনস্টলেশন এবং পরিচালনা করুন।

- মজুদ অ্যাপস এবং সংলাপগুলির সতর্কতা সমূহ পরীক্ষা করুন এবং যদি কোনো অ্যাপ বা সংলাপ সন্দেহভাজন হয় তবে তা আপসার ফোন থেকে সরান।

- অজানা স্রোত থেকে অ্যাপস ইনস্টল করার আগে সংশ্লিষ্ট অ্যাপকে সমীক্ষা করুন এবং ব্যবহারকারীদের পরামর্শ এবং রেটিং পরীক্ষা করুন।

আপনার মোবাইল সুরক্ষা রক্ষা করতে, সতর্কতা অবলম্বন করুন এবং ম্যালওয়্যার থেকে নিরাপত্তা নিশ্চিত করতে সঠিক সুরক্ষা প্রয়োজনীয় পদক্ষেপগুলি গ্রহণ করুন।

ইউনিট – ০৬ : কম্পিউটার নেটওয়ার্কের ধারনা

❖ অধ্যায় – ৬.১ : কম্পিউটার নেটওয়ার্ক

কম্পিউটার নেটওয়ার্ক হলো কম্পিউটার সিস্টেম এবং উপকরণের মধ্যে সংযোগ স্থাপনের পদ্ধতি বা পদ্ধতির সমষ্টি। এটি কম্পিউটার সিস্টেমগুলির মধ্যে ডেটা এবং তথ্য পাঠানোর জন্য সংযোগ বা যোগাযোগের সাধারণ পদ্ধতি। নেটওয়ার্ক কম্পিউটার, রাউটার, সুইচ, ফায়ারওয়াল, সার্ভার, ক্লায়েন্ট এবং প্রোটোকল সম্পর্কিত উপকরণগুলির সমন্বয়ে গঠিত হয়।

নেটওয়ার্কের মাধ্যমে ডেটা একটি নোড থেকে আরেকটি নোডে পাঠানো হয়। নেটওয়ার্কের প্রতিটি নোডকে একটি ঠিকানা অনুমতি দেওয়া হয়, যার মাধ্যমে অন্য নোডে ডেটা প্রেরণ করা যায়। এছাড়াও, নেটওয়ার্কের জন্য প্রোটোকল ব্যবহার করা হয়, যা নেটওয়ার্কের বিভিন্ন পার্টিশনে ডেটা পাঠানোর নির্দেশিকা নিয়ে থাকে।

এই প্রোটোকলগুলি সাধারণত ইতিমধ্যে পরিচিত প্রোটোকল স্ট্যাক ব্যবহার করে, যেমন TCP/IP প্রোটোকল স্ট্যাক।

নেটওয়ার্কে কম্পিউটারের মধ্যে ডেটা পাঠানোর জন্য বিভিন্ন প্রোটোকল ব্যবহার হয়, যেমন IP (আইপি), ICMP (আইসিএমপি), TCP (টিসিপি), UDP (ইউডিপি) ইত্যাদি। এছাড়াও অন্যান্য প্রোটোকলগুলি ব্যবহার করে নেটওয়ার্ক পরিচালনা এবং সুরক্ষা করা হয়।

নেটওয়ার্ক এবং সাইবার সুরক্ষা বিষয়ে আরও বিস্তারিত জানতে, আপনি নেটওয়ার্কিং এবং সাইবার সুরক্ষা সম্পর্কিত বই এবং অনলাইন সোর্স থেকে তথ্য সংগ্রহ করতে পারেন। এছাড়াও, নেটওয়ার্ক প্রশিক্ষণের জন্য পেশাদার কোর্স ও সার্টিফিকেশন কোর্স উপলব্ধ আছে, যা আপনাকে আরও উন্নত স্তরের জ্ঞান এবং দক্ষতা সরবরাহ করতে সাহায্য করবে।

❖ অধ্যায় – ৬.২ : নেটওয়ার্কিং ডিভাইস

নেটওয়ার্কিং ডিভাইস হলো সংযোগ স্থাপনের জন্য ব্যবহৃত সাধনের সমষ্টি যা কম্পিউটার নেটওয়ার্কের মাধ্যমে ডেটা পাঠানো বা গ্রহণ করার জন্য ব্যবহৃত হয়। নেটওয়ার্কিং ডিভাইস বিভিন্ন আকার এবং সাধনের সমন্বয়ে গঠিত হয়ে থাকে, যাতে নেটওয়ার্কে সংযোগ স্থাপন এবং সম্প্রচার পদ্ধতির জন্য উপযুক্ত সাধন সরবরাহ করতে পারে।

কিছু প্রধান নেটওয়ার্কিং ডিভাইসের উদাহরণ হলো:

1. রাউটার: রাউটার নেটওয়ার্কের জন্য মূল গেটওয়ে হিসাবে কাজ করে এবং ডেটা পদ্ধতিগুলির মধ্যে বিভিন্ন নেটওয়ার্কের মধ্যে ডেটা পাঠানো ও রিসিভ করা হয়।
2. সুইচ: এটি নেটওয়ার্কে ডেটা ফ্রেম প্রেরণ এবং গ্রহণের জন্য ব্যবহৃত হয়, এবং মাল্টিপল ডিভাইসের মধ্যে সংযোগ স্থাপনের জন্য ব্যবহৃত হয়।
3. হাব: হাব একটি নেটওয়ার্কিং ডিভাইস যা ডেটা ফ্রেমগুলি মাল্টিপল পোর্টে বিতরণ করে।
4. মডেম: মডেম কম্পিউটারের জন্য ইন্টারনেট সংযোগ স্থাপনে ব্যবহৃত হয়। এটি ইথারনেট বা ব্রডব্যান্ড কানেকশান থেকে সিগন্যাল সংগ্রহ করে এবং সেগুলি কম্পিউটারের জন্য ব্যবহারযোগ্য করে।
5. নেটওয়ার্ক এডাপ্টার: নেটওয়ার্ক এডাপ্টার কম্পিউটারের সাথে নেটওয়ার্ক সংযোগ স্থাপনের জন্য ব্যবহৃত হয়। এটি কম্পিউটারের নেটওয়ার্ক ইন্টারফেস এবং নেটওয়ার্কের সাথে সংযোগ স্থাপন করার জন্য ব্যবহৃত হয়।

নেটওয়ার্কিং ডিভাইস নেটওয়ার্কের মাধ্যমে ডেটা প্রেরণ এবং গ্রহণ করতে ব্যবহৃত হয়, যাতে কম্পিউটার এবং অন্যান্য ডিভাইসগুলি নেটওয়ার্কে সংযুক্ত থাকে এবং তথ্য পাঠানো যায়। নেটওয়ার্কিং ডিভাইস নেটওয়ার্ক সংযোগ প্রতিষ্ঠান এবং ব্যবহারকারীদের মধ্যে সমন্বয় বা ডেটা প্রসারণ করার জন্য মাধ্যম সরবরাহ করে। এই ডিভাইসগুলি প্রকাশিত নেটওয়ার্ক প্রোটোকলগুলি অনুসরণ করে এবং ডেটা পাঠানোর জন্য নির্দিষ্ট নেটওয়ার্ক স্তরে কার্যকর হয়।

❖ অধ্যায় – ৬.৩ : ইন্টারনেট ?

ইন্টারনেট হলো একটি বৃহৎ জালানুসার কম্পিউটার নেটওয়ার্ক যা বিশ্বব্যাপী যুক্ত করে। এটি কম্পিউটার এবং যুক্তিসম্পন্ন ডিভাইসের মধ্যে তথ্য প্রসারণের জন্য ব্যবহৃত হয়। ইন্টারনেট দ্বারা মানুষেরা তথ্য অনুসন্ধান করতে, ইমেল পাঠাতে, সামাজিক যোগাযোগ করতে, ভিডিও দেখতে, অনলাইনে কেনাকাটা করতে, গেম খেলতে, ব্লগ লিখতে এবং অন্যান্য বিভিন্ন কাজে লোকেরা ইন্টারনেট ব্যবহার করে।

ইন্টারনেট প্রথমে যুক্তিসম্পন্ন কম্পিউটার নেটওয়ার্কের মাধ্যমে প্রসারিত হয়। এরপর প্রোটোকলগুলি (যেমন TCP/IP) ব্যবহার করে ডেটা প্রসারিত করা হয়। ইন্টারনেটের জন্য বিশ্বব্যাপী নেটওয়ার্ক ইন্টারকনেক্টেড হয়, যা সাধারণত ক্যাবল, ফাইবার অপটিক কেবল এবং বিভিন্ন নির্দিষ্ট নেটওয়ার্কিং উপাদানের মাধ্যমে হয়। ইন্টারনেটের সংযোগ প্রদানের জন্য ইন্টারনেট সেবা প্রদানকারী (ইন্টারনেট প্রবাহমান প্রদাতা বা ISP) দ্বারা সরবরাহ করা হয়।

ইন্টারনেটের জন্য ব্যবহৃত প্রকৃতি প্রোটোকলগুলির মধ্যে সর্বাধিক পরিচিত হলো ট্রান্সমিশন কন্ট্রোল প্রোটোকল (TCP) এবং ইন্টারনেট প্রোটোকল (IP)। এদের সমন্বয়ে তথ্য সঠিকভাবে পাঠানো হয় এবং ইন্টারনেটের পাঠক, গ্রাহক এবং সার্ভারগুলির মধ্যে সমন্বয় সম্পন্ন হয়। আরও অনেক প্রোটোকল ও প্রোটোকল স্ট্যাক ইন্টারনেটে ব্যবহৃত হয়, যা বিভিন্ন উপযুক্তিগুলি প্রদান করে যেমন হাইপারটেক্সট ট্রান্সফার প্রোটোকল (HTTP), ডোমেন নাম সার্ভিস (DNS), ইমেল প্রোটোকল (SMTP), ইন্টারনেট সংযোগ প্রোটোকল (ICP), সিকিউর সকেট লেয়ার (SSL) ইত্যাদি।

ইন্টারনেট অসংখ্য সেবা সরবরাহ করে, যেমন ওয়েব ব্রাউজিং, ইমেল, অনলাইন চ্যাট, সামাজিক যোগাযোগ, ভিডিও স্ট্রিমিং, অনলাইন শপিং, অনলাইন ব্যাংকিং, মাল্টিমিডিয়া সেবা, গেমিং, বিজ্ঞাপন, সার্ভার হোস্টিং, সাইবার নিরাপত্তা ইত্যাদি। ইন্টারনেটের উপযুক্তিগুলি প্রচুর, সুসংগঠিত এবং দ্রুত বিকাশ করা হচ্ছে যাতে মানুষেরা সরাসরি যেকোনো তথ্য, সেবা এবং সংযোগ পেতে পারেন।

❖ অধ্যায় – ৬.৪ : আইপি অ্যাড্রেস কি ?

আইপি অ্যাড্রেস (IP address) হল একটি সংখ্যার সিরিজ যা ইন্টারনেট প্রোটোকল (IP) ব্যবহার করে নেটওয়ার্কের ডিভাইসে অ্যাসাইন করা হয়। এটি একটি ইউনিক আইডেন্টিফায়ার করণীয় যা নেটওয়ার্ক কমিউনিকেশনের সময় ডিভাইসগুলির মধ্যে তথ্য পাঠানোর জন্য ব্যবহার হয়।

আইপি অ্যাড্রেস দুই প্রকারের হতে পারে:

1. IPv4: IPv4 হল ইন্টারনেটের প্রাথমিক প্রটোকল এবং সর্বপ্রচলিত হয়ে থাকে। এটি 32 বিট দ্বারা প্রকাশিত হয় এবং প্রতিটি বিটকে দশমিক সংখ্যায় প্রকাশ করে। উদাহরণস্বরূপ, 192.168.0.1 একটি IPv4 অ্যাড্রেস।

2. IPv6: IPv6 হল একটি নতুন প্রটোকল যা IPv4 এর পরিবর্তে ব্যবহার করা হয়। এটি 128 বিট দ্বারা প্রকাশিত হয় এবং প্রতিটি বিটকে হেক্সাডেসিমাল সংখ্যায় প্রকাশ করে। উদাহরণস্বরূপ, 2001:0db8:85a3:0000:000

0:8a2e:0370:7334 একটি IPv6 অ্যাড্রেস।

আইপি অ্যাড্রেস ব্যবহার হয় ডিভাইসের একটি আইডেন্টিটি হিসাবে, যাতে সার্ভার ও ক্লায়েন্ট মধ্যে সংযোগ স্থাপন করা যায়।

❖ অধ্যায় – ৬.৫ : আইপি অ্যাড্রেস কিভাবে অনুসন্ধান করা হয় ?

আইপি অ্যাড্রেস অনুসন্ধান করার জন্য আপনি অনলাইনের পরিসর থেকে বিভিন্ন সার্ভিস ও উপায় ব্যবহার করতে পারেন। নিম্নে কিছু উপায় উল্লেখ করা হলো:

1. IP Lookup Tools: আপনি অনলাইনে বিভিন্ন IP লুকাপ টুলগুলি ব্যবহার করে আইপি অ্যাড্রেস অনুসন্ধান করতে পারেন। কিছু জনপ্রিয় IP লুকাপ সার্ভিসগুলি হল: IP2Location, WhatIsMyIPAddress, IPinfo, ইত্যাদি। আপনি এই সার্ভিসগুলির ওয়েবসাইটে গিয়ে আইপি অ্যাড্রেস টাইপ করে অনুসন্ধান করতে পারেন।

2. Command Prompt বা Terminal: আপনি উইন্ডোজে Command Prompt এবং ম্যাক ও লিনাক্সে Terminal ব্যবহার করেও আইপি অ্যাড্রেস অনুসন্ধান করতে পারেন। টার্মিনালে আপনার কম্পিউটারের অপারেটিং সিস্টেমে উপলব্ধ নির্দিষ্ট কমানাগুলি ব্যবহার করে আইপি অ্যাড্রেস অনুসন্ধান করা যায়। উদাহরণস্বরূপ, উইন্ডোজে আপনি `ipconfig` কমান্ড ব্যবহার করতে পারেন

এবং ম্যাক ও লিনাক্সে `ifconfig` কমান্ড ব্যবহার করতে পারেন। এই কমানাগুলি চালানোর মাধ্যমে আপনার কম্পিউটারের নেটওয়ার্ক ইন্টারফেসের সমস্ত তথ্য ও আইপি অ্যাড্রেস দেখতে পারবেন।

এছাড়াও, একটি ওয়েব ব্রাউজারে "আইপি অ্যাড্রেস চেক" অথবা "আইপি অ্যাড্রেস লুকাপ" টাইপ করে সার্চ করলে আপনি বিভিন্ন ওয়েবসাইট থেকে সরাসরি আইপি অ্যাড্রেস অনুসন্ধান করতে পারেন। এই ওয়েবসাইটগুলি আপনাকে আপনার ব্রাউজারের আইপি অ্যাড্রেস দেখাবে।

ইউনিট – ০৭ : ডার্ক-ওয়েব, ডিপ-ওয়েব ও সার্ফেস-ওয়েব

❖ অধ্যায় – ৭.১ : Tor Brwoser

Tor Brwoser সম্পর্কে বিস্তারিত বলেন?

Tor Browser হল একটি ব্রাউজার যা গোপনীয়তার মানদণ্ডে বিশ্বাস করে। এটি একটি মজার উপকরণ, যার মাধ্যমে আপনি ইন্টারনেটে গুপ্তচর হিসাবে সংযুক্ত হতে পারেন। টর ব্রাউজারটি নিজেকে গোপনীয়তার উপরে প্রশাসন করে এবং আপনার গোপনীয় তথ্য এমনভাবে প্রেরণ করে যে এটি দ্বারা এখনও আপনার পরিচালিত স্থান বা আপনার সংযুক্ত হয়েছেন সাইটগুলিতে প্রকাশিত হয় না।

টর ব্রাউজারটি আসলে টর (The Onion Router) নামক একটি নেটওয়ার্কের উপরে নির্ভর করে যা আপনার গোপনীয়তা ও অনুদেশের প্রশাসন করে। এটি আসলে আপনার ইন্টারনেট সংযোগকে পার্শ্ববর্তী সার্কিটে বদলে দেয় যাতে আপনার গোপনীয়তা বজায় রাখা যায়।

টর ব্রাউজারটি একটি মজার ব্যবহারকারী ইন্টারফেস প্রদান করে, যা বিভিন্ন প্রকারের সংযোগের

সাথে যুক্ত হতে সাহায্য করে। এটি প্রমাণ করে যে আপনি প্রকাশিত সাইটগুলি সম্পর্কে আপনার আসল পরিচয় প্রদান না করে ব্যবহার করছেন এবং আপনি আপনার ক্রমান্বয়ে এখানে অনলাইনে অনুসন্ধান করছেন।

এটি একটি কার্যকর নিজস্ব খোলা সোর্স প্রকল্প যা মূলত এনক্রিপ্টেড ইন্টারনেট ট্রাফিক এবং আপনার পরিচয়কে গোপন রাখার উদ্দেশ্যে তৈরি করা হয়েছে। টর ব্রাউজারটি একটি অভিজ্ঞতামূলক গোপনীয়তা পরিবেশ সরবরাহ করে এবং নেটওয়ার্কে পাঠানো ডেটাগুলি এনক্রিপ্ট করে দেয়। এটি আপনার আসল স্থান ও ইউজার প্রদর্শন তথ্য গোপন রাখার জন্য একটি অনলাইন প্রস্তুতি প্রদান করে।

টর ব্রাউজারটি নিরাপদ, স্থায়ী অবস্থায় রয়েছে এবং বিভিন্ন প্ল্যাটফর্মে ব্যবহারযোগ্য (যেমন Windows, macOS, এবং Linux)। এটি টর নেটওয়ার্কের মাধ্যমে আপনার ইন্টারনেট সংযোগ প্রয়োগ করে, যা আপনাকে সংযোগ করে যায় বিশ্বের বিভিন্ন সার্ভারের মাধ্যমে।

একটি গুরুত্বপূর্ণ বৈশিষ্ট্য হল টর ব্রাউজারে ডিফল্ট ভাষা হিসাবে বাংলা বিদ্যমান, যা ব্যবহারকারীদের প্রথমেই ব্রাউজারের ভাষা সহজেই পরিবর্তন করতে সাহায্য করে।

টর ব্রাউজারটি একটি প্রাথমিক ব্রাউজারের মতোই কাজ করে, তবে এর গুপ্তচরতার কারণে কিছু সাইটগুলি যদি আপনি সাধারণ ব্রাউজার দিয়ে প্রবেশ করেন তবে সেগুলি টর ব্রাউজারের মতো পরিচালিত হতে পারে না। টর ব্রাউজারটি আপনাকে একটি সার্কিট মাধ্যমে প্রয়োগ করে আপনার ইন্টারনেট সংযোগের মাধ্যমে অন্য রাউটিং পদ্ধতির মাধ্যমে প্রবেশ করতে সাহায্য করে।

Tor Brwoser কিভাবে ব্যবহার করবো ?

টর ব্রাউজার ব্যবহার করতে নিম্নলিখিত ধাপগুলি অনুসরণ করতে পারেন:

১. টর ব্রাউজার ডাউনলোড করুন: সবচেয়ে প্রথমে, আপনার ব্রাউজারে টর ব্রাউজার সংস্করণটি ডাউনলোড করুন। আপনি এটি টর প্রকল্পের অফিসিয়াল ওয়েবসাইট (https://www.torproject.org/) থেকে ডাউনলোড করতে পারেন।

২. ইনস্টল করুন: ডাউনলোড সম্পূর্ণ হলে, ডাউনলোড করা ফাইলটি আপনার সিস্টেমে ইনস্টল করুন। ইনস্টলেশন প্রক্রিয়াটি অনুসরণ করুন এবং টর ব্রাউজারটি আপনার কম্পিউটারে সঠিকভাবে স্থাপন করুন।

৩. টর ব্রাউজার আরম্ভ করুন: ইনস্টলেশন সম্পন্ন হলে, টর ব্রাউজারটি আরম্ভ করতে পারেন। এটি আপনার কম্পিউটারের ডেস্কটপ বা অ্যাপস মেনুতে অনুপ্রবেশ করবে।

৪. টর ব্রাউজার ব্যবহার করুন: টর ব্রাউজার আরম্ভ করলে, আপনি এখন টর ব্রাউজারের মধ্যমে ইন্টারনেটে গুপ্তচরভাবে সংযুক্ত হতে পারেন। টর ব্রাউজারটি আপনাকে টর নেটওয়ার্কের মাধ্যমে সার্কিট প্রয়োগ করে আপনার গোপনীয়তা বজায় রাখে। টর ব্রাউজারে আপনি ইন্টারনেট ব্রাউজ করতে পারেন এবং গোপনীয়তার সংযোজনে আপনার সংযুক্তি নিয়ন্ত্রণ করতে পারেন।

এই পদক্ষেপগুলি অনুসরণ করে আপনি টর ব্রাউজার ব্যবহার করতে পারবেন। মনে রাখবেন যে, টর ব্রাউজারটি গোপনীয়তার জন্য ব্যবহার করা হয়, কিন্তু এটি সম্পূর্ণ অনিয়মিত কার্যকর উপায়ে পরিচালিত হয় না। তাই অনুগ্রহ করে সতর্কতা অবলম্বন করে এবং সার্বিক গোপনীয়তার প্রয়োজনীয় নীতিমালা মেনে চলুন।

❖ অধ্যায় – ৭.২ : ডার্ক ওয়েব

ডার্ক ওয়েব বা ডার্কনেট হল এমন একটি সেগমেন্ট যা ইন্টারনেটের একটি অংশ এবং পাবলিকভাবে অ্যাক্সেসযোগ্য নয়। এটি গোপনীয়ভাবে সংক্রান্ত ওয়েবসাইটগুলির মধ্যে রয়েছে, যা কার্যকর সরকারী পরিচালনা, অপরিচিত বিক্রয় ও সেবার জন্য ব্যবহার করা হয়।

ডার্ক ওয়েবে অ্যাক্সেস পাওয়ার জন্য আপনার ডার্ক ওয়েব ব্রাউজার ব্যবহার করতে হবে। নীচের ধাপগুলি অনুসরণ করে আপনি ডার্ক ওয়েব ব্রাউজার ব্যবহার করতে পারবেন:

১. ডার্ক ওয়েব ব্রাউজার ডাউনলোড করুন: আপনার পছন্দসইট ডার্ক ওয়েব ব্রাউজারটি সংগ্রহ করুন। কিছু জনপ্রিয় ডার্ক ওয়েব ব্রাউজারের মধ্যে Tor Browser, Freenet, I2P ইত্যাদি রয়েছে। সেগুলি সংগ্রহ করতে অনলাইনে অনুসন্ধান করুন এবং ডাউনলোড করুন।

২. ব্রাউজারটি ইনস্টল করুন: ডাউনলোড সম্পূর্ণ হলে, ব্রাউজারটি ইনস্টল করুন। ইনস্টলেশন প্রক্রিয়াটি অনুসরণ করুন এবং সঠিকভাবে ব্রাউজারটি ইনস্টল করুন।

৩. ডার্ক ওয়েবে অ্যাক্সেস করুন: ডার্ক ওয়েব ব্রাউজারটি আরম্ভ করলে, আপনি ডার্ক ওয়েবে অ্যাক্সেস করতে পারবেন। ব্রাউজারটি আপনাকে ডার্ক ওয়েব সাইটগুলির তালিকা দেখাবে এবং আপনি সেখানে প্রবেশ করতে পারবেন।

ডার্ক ওয়েব ব্রাউজার ব্যবহারের সময় মনে রাখবেন যে, ডার্ক ওয়েব গোপনীয়তা বিষয়ক বিশেষজ্ঞদের জন্য পরামর্শ করা হয়। সতর্কতা অবলম্বন করে এবং অনুগ্রহ করে কেবল আপনার জ্ঞাত এবং বিশ্বস্ত সমস্ত সাইটগুলি পরিচালনা করুন।

❖ অধ্যায় – ৭.৩ : ডিপ-ওয়েব

ডিপ ওয়েব হল দীর্ঘস্থায়ী অল্প গোপনীয়তার ওয়েব সেগমেন্ট, যেখানে ব্যবহারকারীর পরিচালিত গোপনীয় তথ্য সংরক্ষণ করা হয়। ডিপ ওয়েবে তথ্য সংগ্রহ করা, কমিউনিকেশন করা এবং অনলাইনে অপারেশন সম্পাদন করা যায় তবে সেগমেন্টগুলি একটি নেটওয়ার্কের মাধ্যমে অ্যাক্সেসযোগ্য নয়।

ডিপ ওয়েবে অ্যাক্সেস করতে নিম্নলিখিত ধাপগুলি অনুসরণ করতে হবে:

1. ডিপ ওয়েব ব্রাউজার ডাউনলোড করুন: প্রথমে ডিপ ওয়েব ব্রাউজারটি সংগ্রহ করুন। কিছু জনপ্রিয় ডিপ ওয়েব ব্রাউজারের মধ্যে Tor Browser, Freenet, I2P রয়েছে। এই ব্রাউজারগুলি অনলাইনে খোঁজ করুন এবং ডাউনলোড করুন।

2. ব্রাউজারটি ইনস্টল করুন: ব্রাউজারটি ডাউনলোড করার পরে, সঠিকভাবে ইনস্টল করুন। ইনস্টলেশন প্রক্রিয়াটি সহজ হওয়া উচিত এবং সঠিকভাবে পরিচালিত হওয়া উচিত।

3. ডিপ ওয়েবে অ্যাক্সেস করুন: ব্রাউজারটি ইনস্টল করার পরে, ব্রাউজারটি আরম্ভ করুন এবং পরিচিত ডিপ ওয়েব সাইটগুলির তালিকা পেতে পারেন। সেখানে প্রবেশ করতে পারবেন এবং গোপনীয়তা সংরক্ষণ করতে পারবেন। ডিপ ওয়েবে অ্যাক্সেস করতে সাবলীলতা এবং প্রয়োজনীয় সম্মতিপ্রাপ্ত নীতিমালা অনুসরণ করুন।

এটি মনে রাখবেন যে ডিপ ওয়েবে অনন্য নেটওয়ার্ক প্রোটোকলগুলি ব্যবহার করা হয় এবং এটি একটি অংশ যা গোপনীয়তা ও অনলাইন গোপনীয়তা সংরক্ষণ প্রয়োজন করে। ব্যবহারকারীদের কাছে সাবলীলতা ও প্রয়োজনীয় সম্মতিপ্রাপ্ত নীতিমালা অনুসরণ করা উচিত।

❖ অধ্যায় – ৭.৪ : সার্ফেস-ওয়েব

সার্ফেস-ওয়েব হল সাধারণত সকলের কাছে অ্যাক্সেসযোগ্য ওয়েব। এটি আমরা দৈনন্দিন জীবনে ব্যবহার করে থাকি যেমন সামাজিক নেটওয়ার্ক, ই-কমার্স সাইট, ব্লগ, খবর ও বিনোদন ওয়েবসাইট, অনলাইন সেবা প্রদানকারী সাইট ইত্যাদি। এটি সরাসরি পাবলিক ইন্টারনেট থেকে অ্যাক্সেস করা যায় এবং সাধারণ ওয়েব ব্রাউজার ব্যবহার করে সেগুলি প্রদর্শন করা হয়।

সার্ফেস-ওয়েব ব্যবহার করতে নিম্নলিখিত পদক্ষেপগুলি অনুসরণ করতে হবে:

1. ওয়েব ব্রাউজার উদ্ধৃত করুন: প্রথমে আপনার পছন্দসই ওয়েব ব্রাউজার উদ্ধৃত করুন। জনপ্রিয় ব্রাউজারগুলির মধ্যে Chrome, Firefox, Safari, এবং Edge রয়েছে। যদি আপনার কম্পিউটারে ইনস্টল করা না থাকে, তবে অ্যাপস্টোর বা গুগল প্লে স্টোর থেকে আপনার মোবাইল ডিভাইসের জন্য ডাউনলোড করুন।

2. ওয়েবসাইট প্রবেশ করুন: পছন্দমত ওয়েবসাইটে প্রবেশ করতে ব্রাউজারের ঠিকানাবদ্ধতার বাক্সে ওয়েবসাইটের URL লিখুন এবং এন্টার চাপুন। এটি ওয়েবসাইটের মূল পৃষ্ঠার প্রদর্শন করবে।

3. ওয়েবসাইট ব্রাউজ করুন: এখন আপনি ওয়েবসাইটের পৃষ্ঠাগুলি স্ক্রল করে ব্রাউজ করতে পারেন, লিঙ্কে ক্লিক করতে পারেন, পোস্ট পড়তে পারেন, ভিডিও দেখতে পারেন ইত্যাদি। সার্ফেস-ওয়েব এর বিশেষ প্রয়োজন নেই, আপনি সাধারণত ওয়েবসাইটের বিভিন্ন বৈশিষ্ট্যগুলি ব্যবহার করতে পারবেন।

সার্ফেস-ওয়েব একটি পাবলিক ওয়েব হিসাবে সকলের ব্যবহারের জন্য উপযুক্ত এবং অ্যাক্সেস সহজ। এটি আপনাকে প্রায়শই ব্রাউজ করতে দেয় আপনার সাধারণ ওয়েব ব্রাউজার ব্যবহার করে। তবে, সবসময় সতর্ক থাকুন এবং প্রাইভেসি এবং সুরক্ষা সংক্রান্ত সঠিক পরামর্শ অনুসরণ করুন।

❖ অধ্যায় – ৭.৫ : মারিয়ানাস ওয়েব

মারিয়ানাস ওয়েব হল একটি নেটওয়ার্ক সিস্টেম যা গোপনীয়তা ও অনলাইন গোপনীয়তা সংরক্ষণের উদ্দেশ্যে তৈরি করা হয়েছে। এটি একটি সংক্ষিপ্ত নাম যা "কাসকেডিং স্টাইলশিট প্রক্সি" বুঝায়। মারিয়ানাস ওয়েব ব্রাউজার এবং সার্ভারের সংযোগের মাধ্যমে ইন্টারনেট ব্রাউজ করার সময় আপনার গোপনীয়তা ও অনলাইন গোপনীয়তা সংরক্ষণ করে।

মারিয়ানাস ওয়েব সিস্টেমের কাছে প্রথমেই আপনি একটি মারিয়ানাস ওয়েব ব্রাউজার ব্যবহার করেন। এটি ইউজারের ওয়েব ট্রাফিককে একটি মারিয়ানাস ওয়েব সার্ভারের মধ্যে পাঠিয়ে দেয়, যা ট্রাফিক গোপনীয়তা ও অনলাইন গোপনীয়তা সংরক্ষণ করতে সাহায্য করে। এই সার্ভার এটি একটি মারিয়ানাস নোড ব্যবহার করে ইনটারনেটের মধ্যে আপনার ট্রাফিক পরিচালনা করে। নোডগুলি আপনার ইনপুট ডেটা সংরক্ষণ করে এবং আপনার রিকোয়েস্টগুলি প্রক্সি করে এটি ইনটারনেটের মধ্যে প্রেরণ করে।

মারিয়ানাস ওয়েব ব্রাউজার এবং সার্ভারের মধ্যে ক্রিপ্টোগ্রাফিক প্রয়োগ করে ট্রাফিক গোপনীয়তা সংরক্ষণ করে। এটি আপনার ট্রাফিককে এনক্রিপ্ট করে দেয় যাতে তৃতীয় পক্ষ বা মাধ্যম এটি পড়তে পারে না। সার্ভারে প্রাপ্ত ডেটা একটি মারিয়ানাস নোডে প্রেরণ করে, এটি ডিক্রিপ্ট করে এবং শেষতঃ টার্গেটের সাথে সম্পর্ক স্থাপন করার জন্য ওয়েব সার্ভারে প্রেরণ করে। এটি আপনার গোপনীয়তা সংরক্ষণ করার জন্য কঠিনতর ট্র্যাকিং প্রয়োগ সম্ভব করে তৈরি করে।

মারিয়ানাস ওয়েব ব্রাউজার আপনাকে একটি বিশেষ ইন্টারনেট অভিজ্ঞতা প্রদান করে যা আপনার অনলাইন গোপনীয়তা এবং সুরক্ষা সংক্রান্ত সমস্যাগুলি মোচন করতে সাহায্য করে। এটি ওয়েব গোপনীয়তা সংরক্ষণ করার জন্য বিভিন্ন সুরক্ষা মানদন্ড প্রয়োগ করে, যেমন ট্র্যাকিং প্রতিবন্ধী, কুকি মোচন এবং সুরক্ষিত কানেকশন ব্যবহার। এটি একটি গোপনীয় ওয়েব ব্রাউজার হিসাবে পরিচিত এবং ব্যবহারকারীদের গোপনীয়তা ও সুরক্ষা সম্পর্কে বিশ্বাস দেয়।

মারিয়ানাস ওয়েব একটি ওপেন সোর্স প্রকল্প যা বিভিন্ন প্ল্যাটফর্মে ব্যবহার করা যায়, যেমন উইন্ডোজ, ম্যাক, লিনাক্স। এটি গ্রহণযোগ্যতা, সহজ ব্যবহার এবং প্রায়শই পারফরম্যান্সে উত্তেজিত হয় এমন বৈশিষ্ট্যগুলির জন্য জনপ্রিয় হয়েছে। এটি অনলাইন গোপনীয়তা সংরক্ষণে আপনার সাহায্য করতে পারে এবং আপনাকে অনলাইনে নিরাপত্তা ও সুরক্ষাবিধানের জন্য বিশেষ সুবিধা প্রদান করতে সাহায্য করতে পারে।

❖ অধ্যায় – ৭.৬ : হ্যাকিং ডার্ক রুম

হ্যাকিং ডার্ক রুম হল একটি মিথ্যা যা ইন্টারনেটের ভিতরে হ্যাকিং এবং অনৈধ কার্যকলাপের জন্য ব্যবহৃত হয় বলে মনে করা হয়। এটি একটি অনলাইন প্ল্যাটফর্ম বা ফোরাম নয়, বরং এটি সাধারণত অনলাইনের নেতৃত্বে কঠিনভাবে অ্যাক্সেস যায় এবং প্রায়শই আনুষ্ঠানিক হলেও আইনত একটি গুরুত্বপূর্ণ স্থান নয়।

আইনত, হ্যাকিং ডার্ক রুম বা হ্যাকিং ফোরাম ব্যবহার করে হ্যাকাররা নিজস্ব কৌশলগুলি শেখানো এবং অন্যান্য হ্যাকারদের সহযোগিতা পেতে পারেন। এটি হ্যাকিং সংক্রান্ত তথ্য, টুল, রিসোর্স এবং তথ্যবিনিময়ের জন্য একটি মাধ্যম হিসাবে ভালোভাবে ব্যবহৃত হতে পারে। যদিও এটি একটি অনলাইন সাম্প্রদায়িকতার অংশ হিসাবে পরিচিত হতে পারে, কিন্তু এটি অন্যান্য লিগাল ফোরামের সাথে তুলনা করে পর্যাপ্তভাবে প্রাধান্য পায় না।

গুরুত্বপূর্ণ বিষয় হল হ্যাকিং ডার্ক রুম ব্যবহার করা অনৈচ্ছিক কাজ এবং গোপনীয়তার নীতি বহন করেনা। হ্যাকিং ফোরামগুলি অন্যদের অন্ধকারে ধাঁধার মধ্যে এগিয়ে এসে প্রশাসনিক হতে পারে এবং অনৈচ্ছিক কার্যকলাপের জন্য নজরদারি করতে পারে। আরও গুরুত্বপূর্ণ হল মনে রাখা যায় যে হ্যাকিং কার্যকলাপ গ্রাহকের সম্মতি ছাড়াই বিপর্যয়কর এবং বিতর্কযুক্ত হতে পারে, তাই এটি একটি গ্রাহক বা ব্যবহারকারীর জন্য পরামর্শ দেওয়া হয় না।

একটি গোপন দূর্বলতা যে হ্যাকিং ডার্ক রুম সম্পর্কে বৈশিষ্ট্যিকৃত করে, এটি নিশ্চিত করতে গেলে যে কোনও অপ্রত্যাশিত অনুসরণ অথবা অবৈধ কার্যকলাপের মাধ্যমে পূর্বাবস্থা তৈরি করার চেষ্টা হচ্ছে না। হ্যাকিং ডার্ক রুম সম্পর্কে ভ্রান্তি প্রতারণা দেয়া হচ্ছে এবং অন্যান্য গ্রাহকদের তথ্য উপস্থাপন সঠিক নয়। যদিও হ্যাকিং ডার্ক রুম ব্যবহার করে হ্যাকারদের তথ্য এবং সহযোগিতা প্রাপ্ত হতে পারে, তবুও এটি একটি সম্পূর্ণরূপে অপরিষ্কৃত এবং অনুমোদিত পদ্ধতি নয়।

গুরুত্বপূর্ণ হল বিশ্বাস করা হয় না এবং সর্বদা সতর্ক থাকা হয় যে ইন্টারনেটে সার্ভিস করা সাইটের মধ্যে সম্প্রদায়িকতার অন্তর্ভুক্তি অনিচ্ছাকৃত হতে পারে। যদিও কিছু মাধ্যমে হ্যাকিং সংক্রান্ত তথ্য পাওয়া যায়, তবুও এটি সতর্কতা, সুরক্ষা এবং সম্প্রদায়িকতার

বিষয়ে সচেতন থাকা উচিত। অত্যন্ত জরুরি হল কোনও অবৈধ অনুসন্ধান বা কার্যকলাপের অনুমতি প্রদান না করা এবং ইন্টারনেট সম্পর্কে স্বচ্ছতা ও উপস্থাপনা বজায় রাখা।

❖ অধ্যায় – ৭.৭ : সাইবার অপরাধ বাংলাদেশ

সাইবার আইন বাংলাদেশ হলো একটি আইনগত প্রতিষ্ঠান, যা সাইবার সুরক্ষা, ইন্টারনেট ব্যবহার এবং ডিজিটাল পরিচালনা সংক্রান্ত বিষয়বস্তুকে নিয়ন্ত্রণ এবং নিয়ে কানুনের কাছে তল্লিন করে। বাংলাদেশে সাইবার আইনের উদ্দেশ্য হলো সাইবার জগতে অপরাধ প্রতিরোধ এবং ব্যবস্থাপনা করা।

সাইবার আইন বাংলাদেশের প্রধান আইন হলো "সাইবার আইন, ২০০৬"। এই আইন বাংলাদেশে সাইবার অপরাধের সংজ্ঞা ও আপরাধিক দন্ড নির্ধারণ করে। আইনটির অধীনে সাইবার অপরাধের ক্ষেত্রে দণ্ডশূন্যতা নেই এবং অপরাধীদের প্রতিবন্ধী ব্যবস্থা রয়েছে। এছাড়াও আইনটি স্পষ্ট করে বলে থাকে যে, সম্প্রতি সাইবার অপরাধের ক্ষেত্রে দন্ডাদেশ প্রদানের পাশাপাশি নিজস্ব মামলা প্রদত্ত যাবে।

সাইবার আইন বাংলাদেশে কিছু গুরুত্বপূর্ণ বিষয়গুলো বহন করে যা সাইবার অপরাধ এবং সাইবার সুরক্ষা সংক্রান্ত। কিছু উল্লেখযোগ্য বিষয়গুলো নিম্নরূপ:

১. সাইবার অপরাধ: সাইবার অপরাধের অন্তর্ভুক্ত হয় হ্যাকিং, সাইবার পর্যাবেক্ষণ, ডেটা চুরি, অন্যান্য ব্যবসায়িক গোপনীয়তা লঙ্ঘন, সাইবার আপত্তি এবং ইন্টারনেটে অপমানজনক কন্টেন্ট প্রচারের মতো কার্যকলাপগুলো।

২. সাইবার সুরক্ষা: সাইবার সুরক্ষার ক্ষেত্রে সাইবার আইন বাংলাদেশ বিভিন্ন ব্যবসায়িক প্রতিষ্ঠানকে প্রয়োজনীয় নির্দেশ দেয় এবং সাইবার সুরক্ষার প্রক্রিয়াগুলো বিবেচনা করে। এছাড়াও এই আইনের মাধ্যমে সাইবার সুরক্ষা সংক্রান্ত নীতিমালা ও নীতিমালার বাস্তবায়নের জন্য নিয়মগুলো নির্ধারণ করা হয়েছে।

৩. ডিজিটাল পরিচালনা: সাইবার আইন বাংলাদেশ ব্যবহারকারীদের ডিজিটাল পরিচালনা সংক্রান্ত নিয়ম ও বিধিবদ্ধতা সরবরাহ করে। এটি স্বচ্ছন্দে সাইবার প্রকৌশল ব্যবহারের জন্য নির্দেশ দেয়, পরিচালনা করে এবং ব্যবহারকারীদের আইনগত দায়িত্ব ও অবমাননার জন্য নির্দেশ দেয়।

৪. সাইবার ট্রায়াল: সাইবার আইন বাংলাদেশ সাইবার অপরাধের জন্য সাইবার ট্রায়াল প্রদান করে। এটি সাধারণ আইন আদালতের বদলে বিশেষ সাইবার ট্রায়াল কোর্ট প্রতিষ্ঠা করেছে। এই ট্রায়াল কোর্ট সাইবার অপরাধের মামলাগুলো পরিচালনা করতে সক্ষম হয় এবং তাদের নিয়মিত শুনানি ও বিচারের জন্য কর্তৃপক্ষকে প্রশাসনিক ক্ষমতা দেয়।

সাইবার আইন বাংলাদেশে সাইবার অপরাধ এবং সাইবার সুরক্ষার বিষয়ে আরও বিস্তারিত তথ্যের জন্য, আপনি সংশ্লিষ্ট কানুন বা সাইবার আইন বাংলাদেশের আইনগুলোর অনুশন্ধান করতে পারেন বা আইনগত পেশার কর্মকর্তাদের সাথে যোগাযোগ করতে পারেন।

ইউনিট - ০৮ : Shell Upload, Goggle Dork এবং ডেফেজ পেজ কি?

❖ অধ্যায় - ৮.১ : Shell Upload

ওয়েবসাইটে শেল আপলোড করার জন্য একটি কার্যপ্রণালী ব্যবহার করা হয়। নিম্নলিখিত ধাপগুলো অনুসরণ করে শেল আপলোড করা যায়ঃ

1. একটি শেল ফাইল তৈরি করুন: প্রথমে আপনাকে একটি শেল ফাইল (.php, .asp, .jsp, ইত্যাদি) তৈরি করতে হবে। শেল ফাইলটি হ্যাকারের কন্ট্রোল নিতে পারে এবং ওয়েব সার্ভারে কমান্ড এক্সিকিউশন করতে সক্ষম হতে হবে।

2. ওয়েবসাইটে ফাইল আপলোড করুন: এখন আপনাকে ওয়েবসাইটের ফাইল আপলোড মেকানিজম ব্যবহার করে শেল ফাইলটি ওয়েবসাইটে আপলোড করতে হবে। এটি সাধারণত ফাইল আপলোড ফর্ম ব্যবহার করে অথবা ফাইল ট্রান্সফার প্রোটোকল (FTP) ব্যবহার করে হতে পারে।

3. ফাইল এক্সিকিউশন: একবার শেল ফাইলটি ওয়েবসাইটে আপলোড হয়ে গেলে, হ্যাকার শেল ফাইলটি এক্সিকিউট করতে পারে যেটি হয়ে যাবে সার্ভারে কমান্ড রান করা। এতে হ্যাকার অনুমতি পাবে ফাইলের মাধ্যমে সার্ভারে কমান্ড এক্সিকিউশন করতে।

এটি একটি অপ্রতিসামান্যভাবে ম্যালিশাস কার্যকরী পদ্ধতি হিসাবে বিবেচনা করা উচিত। কোনও অন্যকিছুকে অনধিকারগ্রস্ত প্রবেশের চেষ্টা বা অনধিকারগ্রস্ত কাজে ব্যবহার করা সাইবার অপরাধের একটি উদাহরণ। এটি নিয়মিতভাবে সাইবার নিরাপত্তা ও ওয়েব অ্যাপ্লিকেশন সিকিউরিটির জন্য পর্যায়ক্রমে উন্নতি করা উচিত।

9/ **ওয়েবসাইট এ শেল আপলোড করার উদাহরন ?**

শেল ফাইল ওয়েবসাইটে আপলোড করা হলে একটি উদাহরণ হতে পারে একটি কার্যকর সম্পাদক ফাইল আপলোড করার মাধ্যমে। নিম্নলিখিত উদাহরণটি দেখুনঃ

1. একটি ওয়েবসাইটের লগইন ফর্মে যান।

2. লগইন ফর্মে ইনপুট ফার্মটি পরীক্ষা করুন এবং কনসোল মেড দেখুন।

3. লগইন ফর্মে কোনও ফাইল আপলোডের জন্য অ্যাট্রিবিউট আছে কিনা পরীক্ষা করুন। এটি সাধারণত ইনপুট টাইপ 'file' হবে।

4. কোনও শেল ফাইল তৈরি করুন এবং এটির নাম পরিবর্তন করুন যেমন shell.php বা shell.asp।

5. ফাইলটি লগইন ফর্মের ইনপুট ফার্মে আপলোড করুন।

6. সাফল্যের মাধ্যমে ফাইলটি ওয়েবসাইটে আপলোড হয়েছে।

7. এখন আপনি এই শেল ফাইলটি ব্যবহার করে ওয়েবসাইটের নিয়ন্ত্রণ নিতে পারবেন এবং সার্ভারে কমান্ড এক্সিকিউশন করতে পারবেন।

উদাহরণস্বরূপ, হ্যাকার একটি ইমেল সার্ভারের ওয়েবসাইটের লগইন পেজে অ্যাক্সেস পেয়েছে। এই পেজে কনসোলে ফাইল আপলোডের জন্য অ্যাট্রিবিউট আছে যা হ্যাকার দেখেছে। তারপর হ্যাকার একটি শেল ফাইল তৈরি করেছে এবং সেটি ওয়েবসাইটে আপলোড করেছে। এখন হ্যাকার শেল ফাইল ব্যবহার করে ওয়েবসাইটের নিয়ন্ত্রণ নিয়ে সার্ভারে কমান্ড এক্সিকিউশন করতে পারে। এটি হল একটি উদাহরণ যেখানে শেল ফাইল ওয়েবসাইটে সংযোগ করার জন্য ব্যবহৃত হয়েছে।

এটি একটি অপ্রতিসামান্যভাবে ম্যালিশাস কার্যকরী পদ্ধতি হিসাবে বিবেচনা করা উচিত। সাইবার নিরাপত্তা এবং ওয়েব অ্যাপ্লিকেশন সিকিউরিটি সম্পর্কে সচেতনতা বৃদ্ধি করার জন্য সম্ভাব্য প্রতিরোধ ব্যবস্থা নিয়ে কাজ করা উচিত।

❖ অধ্যায় - ৮.২ : ডিফেজ পেজ?

ডেফেন্স পেজ (Defense Page) হল একটি ওয়েবসাইটে প্রতিরোধ বা সাইবার হামলা থেকে সুরক্ষার উদ্দেশ্যে তৈরি করা একটি পৃষ্ঠা। এটি সাধারণত একটি টেম্পোরারি পৃষ্ঠা হয়, যা হ্যাকিং বা অপ্রতিকূল কোনও কার্যকর সামগ্রী বা বিজ্ঞাপনের প্রদর্শনের বিপরীতে থাকে। ডেফেন্স পেজ সাইটের সাধারণ ফাংশনালিটিকে সংক্ষেপে প্রভাবিত করে থাকে এবং সঠিক প্রতিক্রিয়া প্রদানে সাহায্য করে।

ডেফেন্স পেজ একটি ওয়েবসাইটের অংশ হিসাবে বানানো যেতে পারে নিম্নলিখিত ধাপগুলো অনুসরণ করে:

1. ডেফেন্স পেজের প্রথমত উদ্দেশ্য সুরক্ষার জন্য হ্যাকারের প্রবেশকে বাধা দেওয়া। এটি সাধারণত লগইন পেজ বা সাইটের মূল একটি পৃষ্ঠা হিসাবে তৈরি করা যেতে পারে।

2. ডেফেন্স পেজে সাধারণত অস্থায়ী কর্মক্ষমতা থাকে, অর্থাৎ এটি কোনও ইনটারেকশনাল বা সাইটের মূল কনটেন্ট পরিবর্তন করে না। তারা কয়েকটি সাধারণত নির্দিষ্ট তথ্য প্রদান করে যা সাইট ব্যবহারকারীদের সাইটে সঠিক প্রতিক্রিয়া নিতে সাহায্য করে।

3. ডেফেন্স পেজ ক্রিয়েটিভ হতে পারে এবং ব্যবহারকারীদের মনোনিবেশ দিতে পারে। সেটি সাধারণত হ্যাকিং প্রতিক্রিয়ায় আঘাত পাওয়া ব্যবহারকারীদের ভাল মনে করে কাজ করে।

4. ডেফেন্স পেজ সাধারণত বিকল্প রাস্তা প্রদর্শন করে যা অস্থায়ী সাধারণ সেবা ব্যবহারকারীদের অনুপ্রবেশের জন্য পুনঃনির্দেশ করে।

ডেফেন্স পেজগুলি সাধারণত উন্নত ওয়েব সার্ভার কনফিগারেশন বা ওয়েবসাইট এপ্লিকেশনের একটি অংশ হিসাবে বানানো হয়। এটি অনেকগুলি ভাষায় পরিচিত, যেমন PHP, ASP, JSP ইত্যাদি এবং সাধারণত সার্ভারে স্থাপিত হয়। ডেফেন্স পেজে সাধারণত অতিরিক্ত সুরক্ষা প্রমাণ করার জন্য বিশেষভাবে কনফিগার করা হয়, যা সাইবার হামলা থেকে সাইটকে প্রতিরোধ করে।

❖ অধ্যায় - ৮.৩ : Goggle Dork

```
site:docs.google.com inurl:"/d/" "example.com"
site:onedrive.live.com "example.com"
site:dropbox.com/s "example.com"
site:box.com/s "example.com"
site:dev.azure.com "example.com"
site:http://sharepoint.com "example.com"
intext:"ArcGIS REST Services Directory" intitle:"Folder: /"
inurl:"/login.aspx" intitle:"user"
RE: inurl:/wp-content/uploads/wpo_wcpdf
inurl:"/login.aspx" intitle:"adminlogin"
intitle:"PaperCut login"
Re: inurl:"/admin" intitle:"adminlogin"
inurl:wp-content/uploads/sites
Re: inurl:"/user" intitle:"userlogin"
```

ইউনিট - ০৯ Linux, Termux and Programming

❖ অধ্যায় - ৯.১ Linux

Linux একটি ওয়ার্ড যা একটি প্রকারের ওপেন সোর্স অপারেটিং সিস্টেমকে নির্দেশ করে। এটি কম্পিউটার সিস্টেম এবং সার্ভার এর জন্য একটি পরিষ্কৃত এবং সুসংহত কার্যকরী পরিবেশ প্রদান করে।

লিনাক্স বিশ্বের সবচেয়ে জনপ্রিয় ওপেন সোর্স অপারেটিং সিস্টেম হিসাবে পরিচিত। এটি প্রথমবারের বিশ্বয়োগে (১৯৯১) লিনাস টোরভাল্ডসের পরিচালনায় প্রকাশিত হয়েছিল। লিনাক্সের জন্য ডেভেলপমেন্ট কার্য পরিচালনার জন্য গন্তব্য এবং ভিজন করলেও লিনাক্স প্রজেক্টটি এখন একটি বিশ্বব্যাপী সাম্প্রদায়িক উদ্যোগ হিসাবে বিকাশ পেয়েছে।

লিনাক্স একটি মুক্ত এবং ওপেন সোর্স সফ্টওয়্যার, যা এর বিকাশে বড় বৃদ্ধির কারণে একটি বিশাল সংখ্যক সদস্যদের দ্বারা সমর্থিত হয়েছে। এটি মাল্টিপ্ল প্ল্যাটফর্ম সমর্থিত করে এবং বিভিন্ন ডিস্ট্রিবিউশন (যেমন: Ubuntu, Fedora, Debian, CentOS, etc.) এ পাওয়া যায়। লিনাক্স কম্পিউটার সিস্টেম, মোবাইল ডিভাইস, এম্বেডেড সিস্টেম, সার্ভার এবং সুপারকম্পিউটারের মতো বিভিন্ন ডিভাইসে ব্যবহার করা যায়।

লিনাক্স একটি স্কেলাবল এবং স্থায়ী প্রযুক্তি প্ল্যাটফর্ম প্রদান করে যা কম্পিউটার পারফরমেন্স এবং সিকিউরিটির প্রযুক্তিগত দিক থেকে জনপ্রিয়। এটি বিভিন্ন উদ্দেশে ব্যবহার করা হয়, যেমন ডেস্কটপ সিস্টেম, ওয়েব সার্ভার, ডাটা সেন্টার, রাউটার, ফায়ারওয়াল, মোবাইল ডিভাইস, গেমিং কনসোল, এম্বেডেড সিস্টেম, এইচএমআইএল কনফিগারেশন সার্ভার এবং আরও অনেক কিছু।

লিনাক্স একটি মডুলার এবং পাওয়ারফুল অপারেটিং সিস্টেম যা ব্যবহারকারীদেরকে বিভিন্ন সুযোগ প্রদান করে, যেমন কমান্ড লাইন ইন্টারফেস (CLI), গ্রাফিকাল ইউজার ইন্টারফেস (GUI), কাস্টমাইজয়েশন অপশন, পারফরমেন্স মনিটরিং টুল, নেটওয়ার্ক কনফিগারেশন সুবিধা, সিকিউরিটি ফিচার, কমিউনিটি সমর্থন এবং অভিজ্ঞতা সম্পন্ন ব্যবহারকারী সম্প্রদায়ের সমর্থন।

সুতরাং, লিনাক্স একটি প্রায় অসীম সম্পদ এবং বিভিন্ন উদ্যোগ ও বিশ্বব্যাপী সম্প্রদায়িক উদ্যোগের জন্য পরিচিত। এটি বিশ্বে একটি প্রধান ভূমিকা পালন করে এবং আরও উন্নত ওপেন সোর্স প্রযুক্তির উন্নয়নের সাথে সম্পর্কিত বিভিন্ন প্রকল্পে অবদান রাখে।

❖ অধ্যায় - ৯.২ Termux

Termux হলো একটি অ্যান্ড্রয়েড অপারেটিং সিস্টেমের জন্য ডিভেলপমেন্ট এনভায়রনমেন্ট যা লিনাক্স পরিবেশের সাধারণ ফাংশনালিটি এবং টুলসেট প্রদান করে। এটি অ্যান্ড্রয়েড ডিভাইসে টার্মিনাল এনভায়রনমেন্ট প্রদান করে যাতে আপনি লিনাক্স কমান্ডগুলি এবং স্ক্রিপ্ট চালাতে পারেন।

টার্মিনালের মাধ্যমে Termux ব্যবহার করে আপনি লিনাক্সের বিভিন্ন কমান্ডগুলি ব্যবহার করতে পারেন, শেল স্ক্রিপ্ট লিখতে পারেন, প্যাকেজ ইনস্টল করতে পারেন এবং নিজের স্ক্রিপ্ট ও টুলস ডেভেলপ করতে পারেন। এছাড়াও Termux এ অ্যাডিশনাল প্যাকেজ ম্যানেজার প্রদান করা হয় যার মাধ্যমে আপনি আরও প্রোগ্রামগুলি ইনস্টল করতে পারেন।

Termux এর মাধ্যমে আপনি একটি পূর্ণাঙ্গ লিনাক্স কম্পিউটার সিমুলেশন করতে পারেন এবং ডিভাইসে ডাইরেক্টরি, ফাইল সিস্টেম এক্সপ্লোর এবং নেটওয়ার্ক সংযোগ পরিচালনা করতে পারেন। এটি পেন টেস্টিং, হ্যাকিং টুলসের ব্যবহার, সার্ভার প্রশিক্ষণ এবং কম্পিউটার নেটওয়ার্ক সিকিউরিটি পরিচালনা সহ বিভিন্ন উদ্দেশ্যে ব্যবহার করা যায়।

এটি একটি পাওয়ারফুল টুল হওয়ার সাথেই সঠিক অনুমতি এবং সতর্কতা সহকারে ব্যবহার করা উচিত। যে কোনও গোপন বা অননুমোদিত কার্যক্রমে এর ব্যবহার করা উচিত নয়। সার্ভারে বা অন্য ব্যক্তির ডিভাইসে অননুমোদিত অ্যাক্সেস প্রকাশ না করতে সাবধান থাকুন।

টারমাক্স ব্যবহার করতে গেলে আপনাকে যে কমান্ডগুলো অবশ্যই জানা লাগবে?

আমরা যখন এন্ড্রয়েডে কোন একটা অ্যাপ ওপেন করতে চাই অথবা অন্য যে কোন একটা ফোল্ডার ওপেন করতে চাই, তখন আমরা কি করি?

আমরা জাস্ট সিম্পলি অ্যাপ এর আইকন ফোল্ডারের আইকন এর উপরে ক্লিক করি,এই আইকনকেই মূলত চিত্র বলা হয়েছে।

আমরা যখন এই অ্যান্ড্রয়েডে যেকোন আইকনের উপর ক্লিক করছি,তখন কিন্তু আমাদের উইন্ডোজ ও অ্যান্ড্রয়েড অপারেটিং সিস্টেমের যে কার্নেল রয়েছে অর্থাৎ লিনাক্স কার্নেল, সেই কারণে কার্নেলে কিন্তু একটা কমান্ড রান হয় যেটা আমরা সাধারণত দেখতে পারিনা।তবে কাজটা মূলত কমান্ডের মাধ্যমেই হয়।

কিন্তু আমরা এটাকে ব্যবহার করে চিত্রের মাধ্যমে বা গ্রাফিক্যাল ইন্টারফেস(GUI) এর মাধ্যমে।

অন্যদিকে কমান্ডলাইন ইন্টারফেস(CLI) হলো এখানে সব ধরনের কাজ গ্রাফিক্যাল ইন্টারফেস এর মাধ্যমে না করে কমান্ডের মাধ্যমে করা হয়।

আমাদের ব্যবহৃত লিনাক্স ডিস্ট্রো গুলোতে আমরা CLI এবং GUI দুটই দেখতে পাই, তবে এখানে CLI এর ব্যাবহার ই বেশি।

টার্মিনাল কি?

একটি লিনাক্স ডিস্ট্রো কে অপারেট করার জন্য আমরা যেই অ্যাপ্লিকেশনে কমান্ডগুলো ইনপুট দিয়ে থাকি এবং প্রয়োগ করে থাকি সেটাকেই বলা হয় টার্মিনাল।

সোজাসুজি বলতে গেলে আমরা কমান্ডগুলো যেখানে লিখি সেটাই হচ্ছে টার্মিনাল।

এখন আসি টারমাক্স এর ব্যপ্যারে

এখন যদি আপনাকে জিজ্ঞেস করা হয় টারমাক্স কি?

টার্মাক্স একটি অ্যান্ড্রয়েড টার্মিনাল এমুলেটর এবং লিনাক্স এনভায়রনমেন্ট অ্যাপ্লিকেশন যা কোনও রুটিং বা সেটআপের প্রয়োজন ছাড়া সরাসরি কাজ করে।

অর্থাৎ টারমাক্স একটা টার্মিনাল যা আপনাকে লিনাক্সের কমান্ডগুলো এক্সিকিউট করার সুযোগ দিচ্ছে আপনার এন্ড্রয়েডের মাধ্যমে।

টারমাক্স আপনি কেউ ইউজ করবেন?

আপনি যদি ইথিক্যাল হ্যাকিং, পেনটেস্টিং ইত্যাদিতে আগ্রহী হয় অথবা আপনি যদি লিনাক্স ডিট্রো এর ব্যাবহার শিখতে চান তাহলেই আপনি টার্মাক্স ব্যাবহার করুন।

এতক্ষণ যা বলেছি তা থেকে হয়তো বুঝতেই পারছেন যে টারমাক্স এ সব কাজ আমাদের কমান্ড এর মাধ্যমে করতে হবে, তো এখন কমান্ড নিয়ে কিছু কথা বলি,

[আপনারা চাইলে নিচের এই অংশটি skip করতে পারেন,তবে কারো ভবিষ্যতে shell scripting শেখার ইচ্ছা থাকলে পড়তে পারেন।

$ rm -rf filename

এটা হলো কোন ফাইল রিমুভ বা ডিলিট করার কমান্ড,

আমরা সাধারণত এর সম্পূর্ণ অংশটাকেই কমান্ড বলে থাকি, কিন্তু আসলে সম্পূর্ণ অংশটাই কমান্ড নয়,

এখানে, rm হচ্ছে কমান্ড, যার দ্বারা remove বুঝায়।

এরপর -rf এটাত কমান্ড না এটাকে বলা হয়- ফ্লাগ,যা কমান্ড কে মডিফাই করে, এখানে -rf দ্বারা force remove বুঝাচ্ছে, নরমালি সব ফাইল আপনি $ rm filename এই কমান্ড দ্বারাই রিমুভ করতে পারি, কিন্তু কিছু ফাইল বা ফোল্ডার রিমুভ করতে বিভিন্ন পারমিশন এর প্রয়োজন হয়, সেইক্ষেত্রে কোন পারমিশন ছাড়া রিমুভ করতে -rf ফ্লাগ ইউজ করা হয়।

আর এরপর filename অর্থাৎ যেই ফাইল রিমুভ করবেন তার নাম লিখবেন, এটাকে বলা হয় আর্গুমেন্ট। কারণ এর মাধ্যমে আপনি মূলত নির্দিষ্ট ফাইল রিমুভ করার শর্ত দিয়ে দিচ্ছেন তাই এটাকে বলা হয় আর্গুমেন্ট

$ rm -rf filename

rm : command

-rf : flag

filename : argument

তো আপাতত আমরা কমান্ড ফ্লাগ আর্গুমেন্ট আলাদা ভাবে ডিফাইন না করে পুরো অংশটাকেই কমান্ড বলল,পোস্ট লেখার বা আপনাদের বোঝার সুবিধার্তে।

[যারা skip করেছেন এখান থেকে পড়া শুরু করেন]

Termux ইন্সটল করার পর আমাদের প্রথমেই আমাদের কার্নেল আপডেট করে নিতে হবে নিম্নোক্ত কমান্ডগুলোর মাধ্যমে-

$ apt update -y

$ apt upgrade -y

আমাদের জানতে হবে প্যাকেজ কি?

সহয ভাষায় package হলো কোন টুলস বা সফটওয়্যার রান করার জন্য প্রয়োজনীয় ফাইল বা তথ্য ইত্যাদির সমাবেশ।

যেমন python একটি প্যাকেজ, যাতে পাইথন এর যেকোন টুলস বা সফটওয়্যার রান করার জন্য সবকিছু থাকে।

টারমাক্স এ প্যাকেজ ইনস্টলেশনঃ

Install package:

$ pkg install [package name]

Remove package:

$ pkg uninstall [package name]

List all packages:

$ pkg list-all

Upgrading packages:

$ pkg upgrade

অর্থ্যাৎ আমরা যদি python প্যাকেজ ইনস্টল করতে চাই আমাদের কমান্ড রান করতে হবে,

$ pkg install python

· আন-ইন্সটল করতে চাইলেঃ

$ pkg uninstall pytho

· একই কাজগুলো আমরা apt (aptitude package mannager) এর মাধ্যমেও করতে পারি।যেমন,

$ apt install python -y

$ apt uninstall python -y

একই ভাবে নিচের প্যাকেজগুলো ইন্সটল করে নিবেন,

$ pkg install git -y

$ pkg install php -y

$ pkg install curl -y

$ pkg install wget -y

$ pkg install figlet -y

$ pkg install ncurses-utils -y

আমরা টারমাক্স এ যেসব টুলস ইউজ করব তার অধিকাংশই হবে python ল্যাঙ্গুয়েজ এ! তাই এই python টুলস গুলো রান করার জন্য আমাদের আরো কিছু বিষয় জানতে হবে।

Python programming language ব্যাবহার করে যখন কোন টুলস তৈরি করা হয় তখন এতে বিভিন্ন modules import করা হয় বা ব্যাবহার করা হয়। (অধিকাংশ প্রোগ্রামিং ল্যাঙ্গুয়েজ এই modules এর ব্যাবহার রয়েছে)

Modules : কোন নির্দিষ্ট কাজ কে বাস্তবায়ন করার জন্য কোড বা ডেটা সংক্ষিপ্ত করণে modules ব্যাবহৃত হয়।

যাক modules নিয়ে পরে বিস্তারিত আলোচনা করা যাবে, আপাতত আমরা জেনে রাখি, টুলস টি তৈরি করার সময় কিছু গুরুত্বপূর্ণ modules import করা হয়ে থাকে যা আমাদের টুলস টি রান করার জন্যও প্রয়োজন হবে।

পাইথন এ বিভিন্ন modules এর সমষ্টিকেও প্যাকেজ বলা হয়ে থাকে। আর পাইথন এর প্যাকেজ ম্যানেজার হলো pip.

তাই আমাদের কে আমাদেরকে আমাদের modules গুলো ইনস্টল করতে হবে pip এর মাধ্যমে। আর তার আগে আমাদের pip আপগ্রেড করে নিতে হতে পারে।

উল্লেখ্য, pip আমাদের আলাদাভাবে ইন্সটল করতে হবে না, python প্যাকেজ ইনস্টল এর সাথে সাথে এটিও ইন্সটল হয়ে যায়।

Upgrade pip and pip2 :

pip install –upgrade pip

pip2 install –upgrade pip

· এবার আমাদের modules গুলো ইন্সটল করতে হবে,

For pip2:-

$ pip2 install mechanize

$ pip2 install requests

$ pip2 install bs4

For pip:-

$ pip install requests

$ pip install mechanize

$ pip install bs4

এখন আপনাকে টারমাক্স এ স্টোরেজ পারমিশন দিতে হবে

$ termux-setup-storage

টারমাক্স এর বেসিক সেটআপ সম্পন্ন হলো

তো টারমাক্স এখন ব্যাবহার এর জন্য প্রস্তুত, এখন আমাদের জানতে হবে যে আমরা এটাকে কিভাবে ব্যাবহার করব।

লেখার ও আপনাদের বোঝার সুবিধার্তে আমি কমান্ড গুলো এভাবে লিখব।

$ command (কমান্ডের ফুলফর্ম) [কমান্ডের কাজ]

$ pwd (present working directory) [আপনি বর্তমানে কোন ফোল্ডার বা ডিরেক্টরিতে এ আছেন তা দেখতে)

$ ls (list files) [আপনি যেই ফোল্ডার লোকেশনে আছেন সেখানে কি কি ফাইল/ফোল্ডার আছে তা দেখতে বা তা লিস্টিং করতে]

· ls

(শুধু ls কমান্ড দিলেই আপনি ফাইল সমূহের লিস্ট দেখতে পারবেন)

· ls folder name

(কোন সাব ডিরেক্টরির ফাইল দেখতে)

$ cd (change directory) [ডিরেক্ট্রি চেঞ্জ করতে]

· cd (যেকোনো ডিরেক্টরি থেকে হোম ডিরেক্টরি তে ফিরে যেতে)

· cd- (আগের ডিরেক্টরিতে ফিরে যেতে)

· cd foldername (নির্দিষ্ট ডিরেক্টরি বা লোকেশনে যেতে)

$ mkdir (make directory) [নতুন ডিরেক্টরি বা ফোল্ডার ক্রিয়েট করতে]

· mkdir dirname

· mkdir dir1 dir2 dir3 dir4 (একসাথে অনেকগুলো ফোল্ডার ক্রিয়েট করতে)

$ rm (remove) [কোন কিছু রিমুভ করতে]

· rm filename (কোন ফাইল রিমুভ করতে)

· rm -rf filename (ফোর্স রিমুভ করতে)

· rm -rf dirname (ডিরেক্টরি বা ফোল্ডারকে ফাইলসহ রিমুভ করতে)

$ touch filename.ext (কোন ফাইল ক্রিয়েট করতে touch ব্যাবহৃত হয়)

· touch test.html (তাহলে test নামের একটি html ফাইল ক্রিয়েট হবে)

$ nano filename.ext (কোন টেক্সট বেজড ফাইল ইডিট করতে nano editor ব্যাবহার করা হয়)

· nano test.html (তাহলে nano ইডিটর এ test.html file টি ওপেন হবে, সেখানে কোন কিছুর লেখার পর তা সেভ করতে CTRL+X চাপলে আপনি সেটা সেভ করবেন কি না তা জানতে যাবে, y প্রেস করে এন্টার এ চাপ দিন, ফাইলটি সেভ হয়ে যাবে

আর ইডিট না করে শুধু ফাইল এর কন্টেন্টস দেখতে চাইলে,

$ nano -v filename

উল্লেখ্য টারমাক্স এ কাজ করার সময়, কোন ফাইলের extention উল্লেখ থাকলে আমাদের ও তা উল্লেখ করে দিতে হবে। যেমন টেক্সট ফাইল হলে filename.txt পিএইচপি ফাইল হলে filename.php

$ cp (copy) [কোন ফাইল/ফোল্ডার কপি করতে]

path : path হলো কোন ফাইল বা ফোল্ডার এর লোকেশন।

মনে করি আমরা এখন Test নামের ডিরেক্টরিতে আছি , এবং সেইখানে আরো একটি ডিরেক্টরি আছে storage নামে, তার ভিতর আরো একটি সাব ফোল্ডার আছে image নামের, তার ভিতর abc.jpg নেমের কোন ইমেজ আছে।

তাহলে তার path হলো : storage/image/abc.jpg

· cp [file path] [destination path]

$ cp storage/image/abc.jpg Test

আবার Test ফোল্ডারের কোন কিছু image folder এ কপি করতে চাইলে,

$ cp filename storage/image

আবার যেকোন ফাইল টারমাক্স এর হোম ফোল্ডারে কপি করতে চাইলে,

$ cp [path] $HOME

অর্থাৎ যেইখানে ফাইল টা আছে তার লোকেশন আগে, আর যেইখানে কপি করতে চান তার লোকেশন পরে, আর আপনি যেই ফোল্ডারে আছেন সেইফোল্ডারেই ফাইল থাকলে লোকেশন না শুধু ফাইলনেম হবে।

$ mv (move) [কোন ফাইল বা ফোল্ডার একস্থান থেকে অন্যস্থানে মুভ করে]

Copy ও Move করার ক্ষেত্রে সব ই সেম হবে শুধু cp এর জায়গায় mv লিখতে হব

বিঃদ্রঃ কোন ফাইল কপি বা মুভ করার সময় যদি permission required এমন লেখা দেখায় তাহলে cp -f / mv -f লিখে ট্রাই করবেন।

এছাড়া mv কমান্ড ইউজ করে ফাইল rename ও করতে পারবেন।

$ mv filename new_filename

ফাইল zip unzip করার জন্য,

$ pkg install zip (zip pkg টি ইন্সটল করতে হবে)

$ zip [zipname] [filename1 filename2 filename3]

মনে করি আমরা test1 test2 test3 নামে তিনটা ফাইল এর zip করতে চাই, আর zip ফাইলের নাম দিব abc,তাহলে কমান্ড হবে-

$ zip abc test1 test2 test3

আর unzip করতে চাইলে,

$ chmod +x filename.zip

$ unzip filename.zip

এইক্ষেত্রে,

$ chmod +x abc.zip

$ unzip abc.zip

কিছু কিছু ফাইলের ক্ষেত্রে আমাদের অর্থ্যাৎ ইউজার এর শুধু read only পারমিশন থাকে, তাই এই ফাইল নিয়ে কাজ করতে চাইলে আমাদের execute করার পারমিশন দিতে হয় chmod +x কমান্ড এর মাধ্যমে, কোন ফাইল এর execute করার পারমিশন থাকলে সেই ফাইলনেম টি সবুজ কালারে দেখাবে

$ git clone (Github repository থেকে কোন কিছু ক্লোন করতে বা ডাউনলোড করাও বলতে পারেন)

· git clone [git link]

$ git clone https://github.com/example

এরজন্য অবশ্যই আপনার git pkg টি ইন্সটল থাকতে হবে।

$ wget (কোন ফাইল ডাউনলোড করতে)

· wget [download link]

টার্মাক্স এ কোন প্রসেস STOP করতে CTRL+C প্রেস করুন, ফোর্স স্টপ করতে CTRL+Z প্রেস করুন।

Session close করতে exit কমান্ড রান করুন!

Termux কমান্ড তালিকা এবং ব্যবহার।

একজন Termux ইউজার এবং হ্যাকার হিসেবে কমান্ডগুলি আপনাকে অবশ্যই আয়ত্ত করতে হবে। এই Termux কমান্ড তালিকা খুব দরকারী, এই আদেশগুলি প্রায়শই অ্যাপ্লিকেশন, ফাইল, ফোল্ডার এবং আরও অনেক কিছু ইনস্টল করতে, পরিচালনা করতে ব্যবহৃত হবে।

১/ প্যাকেজ অনুসন্ধানঃ

নির্দিষ্ট প্যাকেজ অনুসন্ধান করার জন্য pkg search কমান্ড ব্যবহার করা হয়। টার্মাক্স প্যাকেজ অনুসন্ধানের জন্য আপনি pkg search কমান্ডটি ব্যবহার করতে পারেন।

$ pkg search প্যাকেজের নাম

উদাহরণ স্বরূপঃ

$ pkg search metasploit

২/ প্যাকেজ ইনস্টলঃ

pkg install কমান্ডটি বর্তমানে ইনস্টল না থাকা টার্মাক্স প্যাকেজ ইনস্টল করে এবং ইতিমধ্যে ইনস্টল থাকা প্যাকেজ আপডেট করে।

$ pkg install প্যাকেজের নাম

উদাহরণ স্বরূপঃ

$ pkg install metasploit

৩/ প্যাকেজ আনইনস্টলঃ

আনইনস্টল প্যাকেজ কমান্ডটি প্যাকেজ বা কোনও সরঞ্জাম আনইনস্টল করতে ব্যবহৃত হয়। আপনি সহজেই এই আদেশ দ্বারা আপনার Termux থেকে যে কোনও প্যাকেজ আনইনস্টল করতে পারেন।

$ pkg uninstall প্যাকেজের নাম

উদাহরণ স্বরূপঃ

$pkg uninstall metasploit

৪/ টার্মাক্সে একটি প্যাকেজ পুনরায় ইনস্টলঃ

আপনি যদি পূর্বে ইনস্টল করা একই সংস্করণগুলিতে Termux প্যাকেজগুলি পুনরায় ইনস্টল করতে চান তবে আপনি এই আদেশটি ব্যবহার করতে পারেন। Pkg রিইনস্টল কমান্ড প্রথমে আনইনস্টল করবে এবং তারপরে প্যাকেজটি আবার আপনার Termux এ ইনস্টল করবে।

$ pkg reinstall প্যাকেজের নাম

উদাহরণ স্বরূপঃ

$ pkg reinstall metasploit

৫/ প্যাকেজ সম্পর্কে বিস্তারিত তথ্য পানঃ

pkg শো কমান্ড সাধারণত একটি নির্দিষ্ট প্যাকেজ সম্পর্কে বিস্তারিত তথ্য প্রদর্শন করতে ব্যবহৃত হয়। প্যাকেজ সম্পর্কে বিস্তারিত তথ্য পেতে এই কমান্ডটি ব্যবহার করুন।

$ pkg show প্যাকেজের নাম

উদাহরণ স্বরূপঃ

$ pkg show metasploit

৬/ ইনস্টল টার্মাক্স প্যাকেজ তালিকাঃ

আপনার টার্মাক্সে বর্তমানে ইনস্টল থাকা সমস্ত প্যাকেজগুলির তালিকা পেতে এই কমান্ডটি ব্যবহার করুন।

$ pkg-list-installed

৭/ সমস্ত টার্মাক্স প্যাকেজ তালিকাভুক্ত করুনঃ

টেরমাক্সের জন্য উপলব্ধ সমস্ত প্যাকেজগুলির তালিকা পাওয়ার জন্য pkg list-all কমান্ড ব্যবহার করা হয়। সমস্ত উপলব্ধ প্যাকেজগুলির তালিকা দেখতে এই কমান্ডটি ব্যবহার করুন।

$ pkg list-all

৮/ ফাইলগুলির অবস্থান প্রদর্শন করুনঃ

টার্মাক্সে ইনস্টল করা ফাইল এবং প্যাকেজগুলির অবস্থান প্রদর্শন করতে ব্যবহৃত পিকেজি ফাইল। উদাহরণ সহ কমান্ডটি নীচে দেখানো হয়েছেঃ

$ pkg files প্যাকেজের নাম

উদাহরণ স্বরূপঃ

$ pkg files metasploit

□□৯/ আপডেট এবং আপগ্রেড টার্মাক্স প্যাকেজঃ

pkg আপডেট && pkg আপগ্রেড -y হল && দ্বারা পৃথক দুটি কমান্ডের মিশ্রণ। আপনি টার্মাক্সে && যোগ করে টার্মাক্সে একাধিক কমান্ড ব্যবহার করতে পারেন।

প্রথমে pkg আপডেট কমান্ড কার্যকর হবে এবং তারপরে pkg আপগ্রেড কমান্ড কার্যকর হবে। -y হ্যাঁ প্রম্পট করতে ব্যবহৃত হয়।

সহজ কথায়, এই Termux কমান্ডটি আপনার Termux প্যাকেজ আপডেট এবং আপগ্রেড করবে।

$ pkg update && pkg upgrade -y

১০/ Termux স্ক্রিন সাফ করুনঃ

টার্মাক্স স্ক্রিনটি সাফ করতে এই কমান্ডটি ব্যবহার করুন।

$ clear

১১/ বর্তমান ওয়ার্কিং ডিরেক্টরি মুদ্রণ করুনঃ

ওয়ার্কিং ডিরেক্টরি মুদ্রণের জন্য এই টার্মাক্স কমান্ডটি ব্যবহার করুন, এর অর্থ হ' ল কমান্ডটি আপনাকে বর্তমান ডিরেক্টরিতে উপস্থিত একটি ডিরেক্টরি দেবে।

$ pwd

১২/ ডিরেক্টরি পরিবর্তন করুনঃ

ডিরেক্টরিটি পরিবর্তন করতে আপনি এই কমান্ডটি ব্যবহার করতে পারেন। এই কমান্ডটি ব্যবহার করে আপনি সহজেই একটি ডিরেক্টরি থেকে অন্য ডিরেক্টরিতে যেতে পারেন। উদাহরণটি নীচে দেওয়া হল।

$ cd $HOME

$ cd /sdcard

প্রথম কমান্ড আপনাকে Termux হোম ডিরেক্টরিতে নিয়ে যাবে অন্য আদেশ আপনাকে অ্যান্ড্রয়েড ডিভাইসের এসডি কার্ডে নিয়ে যাবে।

১৩/ ডিরেক্টরি থেকে ফিরে যাওয়াঃ

$ cd ..

$ cd ../../

১৪/ বর্তমান ডিরেক্টরি ফাইল এবং ফোল্ডার দেখুনঃ

বর্তমান ডিরেক্টরিতে উপস্থিত ফাইল এবং ফোল্ডারগুলি দেখতে এই Termux কমান্ডটি ব্যবহার করুন।

$ ls

১৫/ লুকানো ফাইল সহ ফাইল এবং ফোল্ডারগুলিঃ

সম্পর্কে আরও তথ্য দেখতে আপনি এই আদেশটিও ব্যবহার করতে পারেন।

$ ls -lha

১৬/ ফাইলগুলি অনুলিপি করুন – cp

একটি ডিরেক্টরি থেকে অন্য ডিরেক্টরিতে ফাইলটি অনুলিপি করতে সিপি ব্যবহার করা হয়। উদাহরণস্বরূপ, আমার কাছে একটি ফাইল রয়েছে যা এসডি কার্ডে উপস্থিত এবং ফাইলটির নাম “ডকুমেন্ট” । এবং আমি নথিটি Termux হোম ডিরেক্টরিতে স্থানান্তর করতে চাই তারপরে নিম্নলিখিত কমান্ডটি ব্যবহার করা হবেঃ

$ cp /sdcard/document $HOME

১৭/ ফাইলগুলি সরান – mv

এমভি কমান্ডটি এক ফোল্ডার থেকে অন্য ফোল্ডারে ফাইল অনুলিপি করতে ব্যবহৃত হয়। কার্যপ্রণালী উপরের হিসাবে কমান্ড মাত্র ব্যবহার একই mv পরিবর্তে CP যদি আপনি ফাইল স্থানান্তর করতে চান।

১৮/ ফাইল এবং ফোল্ডার মুছুনঃ

ডিরেক্টরি বা ফোল্ডারে ফাইলগুলি মুছতে rm ব্যবহার করা হয়। rm -rf ফোল্ডার এবং এর সামগ্রী মুছতে ব্যবহৃত হয়। উদাহরণস্বরূপ, আমি “ডকুমেন্ট” নামে একটি ফোল্ডার মুছতে চাই তারপর আমি সেই ফোল্ডারটি মুছতে নিম্নলিখিত কমান্ডটি ব্যবহার করব।

$ rm -rf ডকুমেন্ট

১৯/ ফাইল এবং ফোল্ডারের অনুমতি পরিবর্তন করুন

chmod কমান্ডটি ফাইল এবং ফোল্ডারের অনুমতি পরিবর্তন করতে ব্যবহৃত হয়। কখনও কখনও কিছু ফাইলের কেবল পড়ার অনুমতি থাকে। রাইটিং পড়তে ও এক্সিকিউট করতে পড়া থেকে কোনও ফাইলের অনুমতি পরিবর্তন করতে আমরা নিম্নলিখিত কমান্ডটি ব্যবহার করবঃ

$ chmod +x ফাইলের নাম এখানে

২০/ একটি ফাইল পড়ুন বা তৈরি করুনঃ

যে কোনও পাঠ্য পড়তে, এইচটিএমএল, পাইথন ফাইল ইত্যাদি বিড়াল কমান্ড ব্যবহার করা হয়। উদাহরণস্বরূপ, আমি "ডকুমেন্ট.টেক্সট" এর সামগ্রীটি পড়তে চাই। তারপরে আমি নিম্নলিখিত কমান্ডটি ব্যবহার করব:

$ cat document.txt

দয়া করে মনে রাখবেন যে যদি ফাইলটি নির্দিষ্ট গন্তব্যটিতে উপস্থিত না থাকে। তারপরে ডকুমেন্ট.টেক্সট ফাইল তৈরি হবে

২১/ জিপ কমান্ড

জিপ হ' ল টার্মাক্সের জনপ্রিয় কমান্ড। এটি একটি নির্দিষ্ট ফাইল বা ফোল্ডার সংকোচনের এবং ডিকম্প্রেস করতে ব্যবহৃত হয়।

ফাইল সঙ্কুচিত করতে নিম্নলিখিত কমান্ডটি ব্যবহার করা হবে:

$ zip ফাইল নাম এখানে

একটি ফাইল সঙ্কুচিত করতে নিম্নলিখিত কমান্ডটি ব্যবহার করা হবে:

$ unzip ফাইল নাম এখানে

দ্রষ্টব্য: জিপ এবং আনজিপ কমান্ডটি ব্যবহার করতে, আপনাকে নিম্নলিখিত টার্মাক্স কমান্ডটি লিখে জিপ ইনস্টল করতে হবে।

$ pkg install zip

২২/ ডিরেক্টরিটি তৈরি করুন এবং সরানঃ

ডিরেক্টরিগুলি তৈরি করতে mkdir কমান্ড ব্যবহার করা হয়, আর rmdir Termux কমান্ড ডিরেক্টরি মুছে ফেলার জন্য ব্যবহৃত হয়।

উদাহরণস্বরূপ, আমি Termux নামে একটি ডিরেক্টরি / ফোল্ডার তৈরি করতে চাই , তারপরে আমি নীচের কমান্ডটি ব্যবহার করব:

$ mkdir Termux

Termux ডিরেক্টরি অপসারণ করতে নিম্নলিখিত কমান্ডটি ব্যবহার করা হবে:

$ mkdir Termux

২৩/ নেটট্যাট কমান্ডঃ

নেটস্ট্যাট কমান্ড এমন ডিসপ্লে উৎপন্ন করে যা নেটওয়ার্কের স্থিতি এবং প্রোটোকল পরিসংখ্যান দেখায়।

$ mkdir Termux

□□২৪/ ডিএফ কমান্ডঃ

নির্দিষ্ট ফোল্ডারে বস্তুর আকার দেখায়।

$ df Termux

২৫/ টার্মাক্স থেকে প্রস্থান করুনঃ

টার্মাক্স বন্ধ করতে এই কমান্ডটি ব্যবহার করুন।

$ exit

২৬/ একটি ফাইল খুলুনঃ

এর সাথে যুক্ত ডিফল্ট অ্যাপ্লিকেশন সহ ফাইলটি খুলুন। উদাহরণস্বরূপ, আমি “readme.txt” ফাইলটি খুলতে চাই। তারপরে আমি নিম্নলিখিত Termux কমান্ডটি ব্যবহার করব:

$ open readme.txt

২৭/ পিং কমান্ডঃ

কোনও নির্দিষ্ট ওয়েব বা আইপি ঠিকানায় ডিভাইসের পুনঃব্যবহারযোগ্যতা নিশ্চিত করার জন্য আইপি ঠিকানা বা কোনও ওয়েবসাইটকে পিং করার জন্য কমান্ডটি ব্যবহৃত হয়। উদাহরণ:

$ open google.com

২৮/ ক্যালেন্ডার দেখানঃ

ক্যালেন্ডারটি দেখানোর জন্য এই কমান্ডটি ব্যবহার করুন।

$ cal

২৯/ শো তারিখঃ

তারিখটি মুদ্রণের জন্য এই আদেশটি ব্যবহার করুন।

$ date

৩০/ কমান্ডের ইতিহাসঃ

আপনি পূর্বে টাইপ করা Termux কমান্ডের ইতিহাস দেখতে এই Termux কমান্ডটি ব্যবহার করুন।

$ history

৩১/ Termux থেকে ফাইল ডাউনলোড করুনঃ

Wget হয় Termux কমান্ড আপনাকে URL থেকে কোনো ফাইল এবং Termux প্যাকেজ ডাউনলোড দেওয়া হবে। এই আদেশের ব্যবহার নীচে উল্লেখ করা হয়েছে:

$ wget ইউআরএল এখানে

এই কমান্ডটি ব্যবহার করতে উইজেট প্যাকেজ ইনস্টল করা দরকার। আপনি নীচের কমান্ডটি ব্যবহার করে উইজেটটি ইনস্টল করতে পারেন:

$ pkg install wget

৩২/ গিট ক্লোন কমান্ডঃ

Github থেকে প্যাকেজগুলি ক্লোন করতে আপনার গিট ক্লোন কমান্ডের প্রয়োজন হবে। এই আদেশের ব্যবহার নীচে উল্লেখ করা হয়েছে:

git clone গিথাবের url এখানে

গিট ক্লোন ব্যবহার করতে, গিট কমান্ডটি টার্মাক্সে ইনস্টল করা আবশ্যক। আপনি নীচের কমান্ডটি লিখে গিট ইনস্টল করতে পারেন।

$ pkg install git

টার্মাক্স ইনস্টল করার পরে আমার কোন প্রাথমিক কমান্ডগুলি টাইপ করা উচিত?

আপনি যখন আপনার অ্যান্ড্রয়েড ডিভাইসে Termux ইনস্টল করেন, Termux কনফিগার করা হয় না এবং আপনি এটি থেকে বেশিরভাগ প্যাকেজ ইনস্টল করতে পারবেন না। Termux এ নিম্নলিখিত বেসিক কমান্ডগুলি লিখে আরও ভাল ব্যবহারের জন্য

আপনাকে অবশ্যই আপনার টার্মাক্সটি কনফিগার করতে হবে।

মূল সংগ্রহস্থল ইনস্টলেশনঃ

নীচের কমান্ডটি আপনার টার্মাক্সে মূল সংগ্রহস্থল ইনস্টল করবে। এই সংগ্রহস্থলটি ইনস্টল করার পরে, আপনি সহজেই মূল সংগ্রহস্থলের মধ্যে উপস্থিত প্যাকেজগুলি ইনস্টল করতে পারেন।

$ pkg install root-repo

অস্থির সংগ্রহস্থল ইনস্টলেশনঃ

নীচের কমান্ডটি আপনার টার্মাক্সে অস্থির সংগ্রহস্থল ইনস্টল করবে। এই সংগ্রহস্থলটি ইনস্টল করার পরে আপনি অস্থির সংগ্রহস্থলগুলিতে উপস্থিত প্যাকেজগুলি সহজেই ইনস্টল করতে পারেন।

$ pkg install উন্সতাব্লে-রেপ

এক্স 11 সংগ্রহস্থল ইনস্টলেশনঃ

নীচের Termux কমান্ডটি আপনার Termux- এ x-11 সংগ্রহস্থল ইনস্টল করবে। এই সংগ্রহস্থলটি ইনস্টল করার পরে, আপনি সহজেই x-11 সংগ্রহস্থলে উপস্থিত প্যাকেজগুলি ইনস্টল করতে পারেন।

$ pkg install x11-repo

টার্মাক্সের জন্য 2.4 সেটআপ স্টোরেজঃ

উপরের কমান্ডটি টার্মাক্সকে আপনার এসডি কার্ডের সঞ্চয়স্থান ব্যবহার করার অনুমতি দেবে। এসডি কার্ড অ্যাক্সেস করার সময় আপনি যে সমস্যার মুখোমুখি হন সেগুলির বেশিরভাগই এই আদেশটি টাইপ করার পরে ঠিক হয়ে যাবে।

$ termux-setup-storage

❖ অধ্যায় – ৯.৩ Programming

ইথিকাল হ্যাকিং হলো একটি কার্যক্রম যেখানে হ্যাকাররা সিস্টেম এবং নেটওয়ার্কের নিরাপত্তা পরীক্ষা করে এবং নিরাপদ রাখার জন্য সিস্টেমের অবস্থানগুলো শেখার চেষ্টা করে। ইথিকাল হ্যাকিং একটি লিগ্যাল কার্যক্রম হিসাবে পরিচিত, যা প্রতিষ্ঠিত প্রতিষ্ঠানগুলো বা সিস্টেম প্রতিষ্ঠানগুলো নিজেদের নিরাপত্তা বিশ্লেষণ এবং পরিক্ষা করার জন্য অনুমোদন দেয়।

Programming এর গুরুত্ব ইথিকাল হ্যাকিং এ অনেকটা মূলত গুরুত্বপূর্ণ। এই ক্ষেত্রে প্রোগ্রামিং প্রয়োগ করে হ্যাকাররা সিস্টেমের সুরক্ষার সফলতার মাধ্যমে সাইবার অপরাধ প্রতিরোধ ও নিরাপত্তা বাড়াতে পারে। ইথিকাল হ্যাকিং করার জন্য প্রোগ্রামিং স্কিলসমূহ প্রয়োজন হয় যেমন নেটওয়ার্ক প্রোটোকল, সিস্টেম সুরক্ষা, ডেটা বাংধারণ ও অ্যাক্সেস সম্পর্কিত জ্ঞান। এছাড়াও প্রোগ্রামিং ব্যবহার করে ইথিকাল হ্যাকাররা নিজেদের আরও কর্মক্ষেত্র বা অপরিচিত নিরাপত্তা নিয়ে কাজ করতে পারেন, যেমন নিরাপত্তা টুলস তৈরি করা, সিস্টেম বুদ্ধিমত্তা উন্নত করা, নিজেদের প্রোগ্রামিং দক্ষতা বাড়ানো ইত্যাদি।

তুলনামূলকভাবে বলতে গেলে, Programming ইথিকাল হ্যাকিং এ একটি প্রাথমিক প্রয়োজনীয়তা, যার মাধ্যমে হ্যাকাররা সিস্টেমের নিরাপত্তা পরীক্ষা করতে এবং নিরাপদ রাখতে সক্ষম হয়। এটি গুরুত্বপূর্ণ স্কিলস এবং জ্ঞানের সংগ্রহের জন্য প্রাথমিক ভূমিকা পালন করে যা হ্যাকাররা তাদের পরবর্তী গুরুত্বপূর্ণ কার্যক্রমে উন্নত করতে পারে।

ইউনিট – ১০ পৃথিবীর সেরা মুসলিম হ্যাকার এবং হ্যাকিং মুভি লিস্ট

❖ অধ্যায় – ১০.১ মুসলিম হ্যাকার

হ্যাকারদের উপাত্ত বা বৈশিষ্ট্য মেটানো খুবই কঠিন এবং সীমাবদ্ধ। তবে মুসলিম হ্যাকারদের মধ্যে কিছু বিশ্বস্ত এবং উল্লেখযোগ্য হ্যাকারদের বিষয়গুলো নিম্নলিখিত হতে পারে:

1. তানেম আলি (Tanmay Bakshi): তানেম আলি একজন কানাডিয়ান হ্যাকার এবং কম্পিউটার সায়েন্স প্রতিষ্ঠানে প্রতিষ্ঠিত কর্মকর্তা। তিনি মেশিন লার্নিং, বিগ ডেটা এবং কৌশল শিখেছেন এবং নতুন প্রযুক্তির মধ্যে উদ্ভাবনী প্রকল্প প্রকাশ করেন। তার বয়স এখনও খুব কম (এখন ১৮) এবং তিনি প্রযুক্তি জগতে বিশ্বস্ত একজন নাম।

2. মাজিদ হাসান (Majid Hussain): মাজিদ হাসান একজন পাকিস্তানি হ্যাকার ও সাইবার সুরক্ষা বিশেষজ্ঞ। তিনি হ্যাকাথন নেটওয়ার্কস নামক একটি ব্যবসা প্রতিষ্ঠান পরিচালনা করেন যা সাইবার সুরক্ষা সংক্রান্ত পরামর্শ ও সেবা সরবরাহ করে। মাজিদ হাসানের প্রয়োজনীয় জ্ঞান এবং দক্ষতা সাইবার সুরক্ষার জন্য প্রশংসিত হয়।

3. কারিম আল-দিন (Karim Baratov): কারিম আল-দিন একজন কাজাখস্তানি মুসলিম হ্যাকার হিসাবে পরিচিত। তিনি একটি আন্ডারগ্রাউন্ড হ্যাকিং গ্রুপের সদস্য ছিলেন এবং আমেরিকান মামলায় গ্রেপ্তার হয়েছিলেন। তিনি একটি গুরুত্বপূর্ণ হ্যাকিং হাক্স প্রশিক্ষণ প্রতিষ্ঠানের মালিক হিসাবে পরিচিত হয়েছিলেন।

4. ইমাদ মোহাম্মদ আলম: বাংলাদেশের একজন হ্যাকার এবং ইসলামী হ্যাকার প্রশিক্ষক। তিনি একটি আন্তর্জাতিক হ্যাকিং সংগঠন "বাংলাদেশ ইসলামিক হ্যাকারস" এর প্রতিষ্ঠাতা।

5. হামজা বেন্দেলেজ: আলজেরীয় একজন জনপ্রিয় হ্যাকার এবং সাইবার সুরক্ষা পেশাদার। তিনি বিভিন্ন সাইবার সুরক্ষা সংস্থা এবং প্রশিক্ষণ প্রোগ্রাম চালিয়ে চলেন।

হামজা বেনদেলাজ নিশান্থ (আরবি : حمزة بن دلاج) একজন আলজেরীয় কম্পিউটার হ্যাকার ও সাইবার-অপরাধী। তিনি Bx1 নামেও পরিচিত। প্রবেশ তথ্য চুরি করে ট্রোজান হর্স নামের স্পাইআই এর সহ-প্রতিষ্ঠাতার ভূমিকা পালন করে তিনি ২০০ আমেরিকান ব্যাংক এবং অর্থনৈতিক প্রতিষ্ঠান এর টাকা স্বয়ংক্রিয় ভাবে তুলে নেন। স্পাইআই অ্যাপলিকেশনটি অন্য হ্যাকারদের কাছে বিক্রি করেন যা স্বয়ংক্রিয়ভাবে কাজ করতে পারে।

বেনদেলাজ বড় হয়েছিল আলজেরিয়ার তিজি ওজু নামক স্থানে, যিনি ১৫ বছর কারারুদ্ধ অবস্থায় ছিলেন এবং ৩ বছর কারামুক্ত (জামিন) হিসাবে ছিলেন।

হামজা বেনদেলাজ এবং রুশ কোডফেন্ডেটকে SpyEye কম্পিউটার ভাইরাস ব্যবহার এবং অমেরিকান ব্যাংক হতে মিলিয়ন ডলার চুরি করার জন্য দণ্ডিত করে অমেরিকান আদালত। তিনি ৮,৫০০ ডলারে SpyEye ভাইরাসের একটি কপি আমেরিকান আন্ডার-কভার অফিসারের কাছে বিক্রি করার সময় প্রথম চিহ্নিত হন। পরে তাকে ২০১৩ সালে থাইল্যান্ডে একটি বিমানবন্দর হতে গ্রেফতার হয় এবং মার্কিন প্রশাসনের কাছে হস্তান্তর করা হয়।

6. ওমার বাখাতির: পাকিস্তানের একজন হ্যাকার এবং ইসলামী হ্যাকার সম্প্রদায়ের প্রতিনিধি। তিনি আন্তর্জাতিক হ্যাকিং ও সাইবার সুরক্ষা কমিউনিটিতে অবদান রাখেন।

7. আমির লিউনি: আমির লিউনি একজন পাকিস্তানি হ্যাকার এবং সাইবার সুরক্ষা বিশেষজ্ঞ। তিনি একটি সাইবার সুরক্ষা সংগঠন "Pakistani Cyber Army" এর প্রতিষ্ঠাতা এবং পরিচালক হিসাবে পরিচিত।

8. বালকানট আরমান: বালকানট আরমান পাকিস্তানের একজন হ্যাকার এবং সাইবার সুরক্ষা বিশেষজ্ঞ। তিনি "Pakistan Haxors Crew" নামক হ্যাকিং সংগঠনের সদস্য।

9. নাদিম বালোচ: নাদিম বালোচ পাকিস্তানের হ্যাকার এবং সাইবার সুরক্ষা পেশাদার। তিনি আন্তর্জাতিক হ্যাকিং সংগঠন "Team Madleets" এর সদস্য।

10. সাইফুদ্দিন আমজাদ: সাইফুদ্দিন আমজাদ বাংলাদেশের একজন জনপ্রিয় হ্যাকার এবং সাইবার সুরক্ষা বিশেষজ্ঞ। তিনি প্রযুক্তি ও সাইবার সুরক্ষা সংক্রান্ত বিভিন্ন প্রতিযোগিতায় অংশ নেন।

11. তারিক মাশদি: তারিক মাশদি বাংলাদেশের একজন বিখ্যাত হ্যাকার এবং সাইবার সুরক্ষা বিশেষজ্ঞ। তিনি আন্তর্জাতিক হ্যাকিং ও সাইবার সুরক্ষা কমিউনিটিতে পরিচিত।

12. হাশিম রাইফউল্লাহ: হাশিম রাইফউল্লাহ বাংলাদেশের একজন হ্যাকার এবং সাইবার সুরক্ষা বিশেষজ্ঞ। তিনি আন্তর্জাতিক সাইবার সুরক্ষা সংস্থা "মুজাহিদিন সাইবার আর্মি" এর সদস্য।

❖ অধ্যায় -১০.২ হ্যাকিং মুভি লিস্ট

এখানে সেরা ১০০ টি হ্যাকিং মুভির একটি তালিকা দেওয়া হলো:

1. "The Matrix" (1999)
2. "Hackers" (1995)
3. "WarGames" (1983)
4. "Sneakers" (1992)
5. "Blackhat" (2015)
6. "Live Free or Die Hard" (2007)
7. "The Girl with the Dragon Tattoo" (2011)
8. "Mr. Robot" (TV Series, 2015-2019)
9. "Untraceable" (2008)
10. "Takedown" (2000)
11. "The Social Network" (2010)
12. "Enemy of the State" (1998)
13. "Tron" (1982)
14. "Ghost in the Shell" (1995)
15. "Ex Machina" (2014)
16. "Algorithm: The Hacker Movie" (2014)
17. "The Italian Job" (2003)
18. "Antitrust" (2001)

19. "Cybergeddon" (2012, Web Series)
20. "Who Am I" (2014)
21. "The Net" (1995)
22. "Source Code" (2011)
23. "Eagle Eye" (2008)
24. "The Fifth Estate" (2013)
25. "Hacker" (2016)
26. "Swordfish" (2001)
27. "Firewall" (2006)
28. "The Bourne Identity" (2002)
29. "Skyfall" (2012)
30. "The Great Hack" (2019, Documentary)
31. "23" (1998)
32. "Black Mirror" (TV Series, 2011-present)
33. "The Thirteenth Floor" (1999)
34. "The Imitation Game" (2014)
35. "Track Down" (2000)
36. "Wargames: The Dead Code" (2008)
37. "Algorithm" (2014)
38. "Die Hard 4.0" (2007)
39. "Antisocial" (2013)
40. "Nerve" (2016)
41. "Disconnect" (2012)
42. "Snowden" (2016)
43. "The Circle" (2017)
44. "The Hacker Wars" (2014, Documentary)
45. "Cypher" (2002)

46. "The Lawnmower Man" (1992)

47. "Control" (2007)

48. "Risky Business" (1983)

49. "The Score" (2001)

50. "The Recruit" (2003)

51. "The Thirteenth Floor" (1999)

52. "The Signal" (2014)

53. "Live Wire" (1992)

54. "Pirates of Silicon Valley" (1999, TV Movie)

55. "Inception" (2010)

56. "The Thirteenth Floor" (1999)

57. "The Girl Who Played with Fire" (2009)

58. "The Congress" (2013)

59. "Firewall" (2006)

60. "Take Down" (2016)

61. "Code 46" (2003)

62. "Reboot" (2012, TV Movie)

63. "The Code" (2009)

64. "Perfect Blue" (1997)

65. "Tron: Legacy" (2010)

66. "The Thirteenth Floor" (1999)

67. "Sneakers" (1992)

68. "Cyberbully" (2011, TV Movie)

69. "The Net 2.0" (2006, Video)

70. "Codebreaker" (2011, Documentary)

71. "Firewall" (2006)

72. "Swordfish" (2001)

73. "We Are Legion: The Story of the Hacktivists" (2012, Documentary)

74. "The Congress" (2013)

75. "TRON: Uprising" (TV Series, 2012-2013)

76. "23: Nichts ist so wie es scheint" (1998)

77. "Algorithm" (2014)

78. "The Net" (1995)

79. "Takedown" (2000)

80. "Black Mirror" (TV Series, 2011-present)

81. "Track Down" (2000)

82. "Pirates of Silicon Valley" (1999, TV Movie)

83. "Who Am I" (2014)

84. "The Girl Who Played with Fire" (2009)

85. "Reboot" (2012, TV Movie)

86. "The Code" (2009)

87. "Perfect Blue" (1997)

88. "Tron: Legacy" (2010)

89. "Cyberbully" (2011, TV Movie)

90. "The Net 2.0" (2006, Video)

91. "Codebreaker" (2011, Documentary)

92. "We Are Legion: The Story of the Hacktivists" (2012, Documentary)

93. "23: Nichts ist so wie es scheint" (1998)

94. "Blackhat" (2015)

95. "Hackers" (1995)

96. "Sneakers" (1992)

97. "WarGames" (1983)

98. "Ghost in the Shell" (1995)

99. "The Thirteenth Floor" (1999)

100. "The Matrix" (1999)

এই তালিকাটি হ্যাকিং ও সাইবার সুরক্ষা নিয়ে মজার ও জনপ্রিয় মুভিগুলো উল্লেখ করে। এই মুভিগুলো হ্যাকিং কিংবা সাইবার সুরক্ষা নিয়ে প্লট এবং কর্মপ্রণালী নিয়ে গড়ে তোলা হয়েছে। আপনি এই মুভিগুলো দেখে হ্যাকিং ও সাইবার সুরক্ষা সম্পর্কে আরও অনেক কিছু জানতে পারেন।

“সিকিউরিটি সিক্রেট হ্যাকবুক” বইটি সম্পর্কে কিছু প্রয়োজনীয় কথা

হ্যাকিং “সিকিউরিটি সিক্রেট হ্যাকবুক” বই হলো এমন একটি বই যা হ্যাকিং বিষয়ে বিস্তারিত তথ্য এবং প্রয়োজনীয় কৌশল সরবরাহ করে। এই ধরনের বই হ্যাকারদের জন্য উপযুক্ত হয় যারা নিজেকে হ্যাকিং বিশ্বে উন্নতি করতে ইচ্ছুক এবং নতুন প্রযুক্তিগুলি শেখার আগ্রহী।

হ্যাকিং “সিকিউরিটি সিক্রেট হ্যাকবুক” বই অনেকগুলি থাকতে পারে এবং তা নির্দিষ্ট বিষয়গুলি প্রকাশ করতে পারে, যেমন হ্যাকিং প্রাথমিক বিষয়গুলি, সাইবার সুরক্ষা, নেটওয়ার্ক পেনেট্রেশন টেস্টিং, ডেটা ফরেনসিক্স, ক্রিপ্টোগ্রাফি, সোশ্যাল ইঞ্জিনিয়ারিং, ওয়েব হ্যাকিং, এথিক্যাল হ্যাকিং ইত্যাদি। এই বইগুলি সাধারণত বিভিন্ন প্রকারের হ্যাকিং তথ্য এবং কার্যকারিতা উপস্থাপন করে যা পাঠকদেরকে এই ক্ষেত্রে সক্ষম করতে সাহায্য করে।

হ্যাকিং “সিকিউরিটি সিক্রেট হ্যাকবুক” বই লেখার জন্য, আপনার নজরদারি ও বিশেষজ্ঞতা প্রয়োজন। বিষয়ে গবেষণা করুন, নতুন প্রয়োগ ও প্রয়োজনীয় কৌশল শেখার জন্য আপনার সময় বিনিয়োগ করুন। একটি ভাল হ্যাকিং হ্যাকবুক বই আপনার লক্ষ্যগুলি অর্জন করার সাথে সাথে আপনাকে উদ্দীপ্ত করবে এবং হ্যাকিং প্রশিক্ষণে আপনাকে আগ্রহী করবে।

পুরো বইটি পরার জন্য আপনাকে অসংখ্য ধন্যবাদ।