

Digitized by
06.03.2021

এথিক্যাল হ্যাকিং ওয়েব অ্যাপ্লিকেশন পেনিট্রেশন টেস্টিং সহজ পাঠ

রুবাইয়াত আকবর



দিব্যিক প্রকাশনী

সূচি

লেখক পরিচিতি	৯
লেখকের কথা	১১
অধ্যায় ০ - পূর্বকথা	১৩
অধ্যায় ১ - তথ্যনিরাপত্তার প্রাথমিক ধারণা	১৭
তথ্যনিরাপত্তা পরিচিতি	১৭
সংকেত ব্যবস্থা	২০
এনক্রিপশন অ্যালগরিদম	২২
নেটওয়ার্ক কমিউনিকেশন	২৮
ওয়েব কমিউনিকেশন	৩৬
অধ্যায় ২ - হ্যাকিংয়ের পরিকল্পনা	৪৩
হ্যাকিংয়ের বিভিন্ন ধাপ	৪৩
নৈতিক বিধিনিষেধ	৫২
পরোক্ষ তথ্য সংগ্রহ	৫৪
প্রত্যক্ষ তথ্য সংগ্রহ	৬৪
অধ্যায় ৩ - প্রস্তুতি পর্ব	৬৯
কালি লিনাক্স	৬৯
লিনাক্সের প্রাথমিক পাঠ	৭৫
হ্যাকিং টুল পরিচিতি	৮৭
টার্গেট মেশিন	৯৬
অধ্যায় ৪ - দুর্বলতা ব্যবস্থাপনা	১০৭
দুর্বলতা বিশ্লেষণ	১০৭
নেটওয়ার্ক স্ক্যানিং টুল	১১০
ওয়েব অ্যাপ্লিকেশন স্ক্যানিং	১৩৫
অধ্যায় ৫ - ওয়েব অ্যাপ্লিকেশন পেনিট্রেশন টেস্টিং	১৫১
ওয়েব আক্রমণের ধারণা	১৫১
ওয়েব আক্রমণ টুল	১৬১
ওয়েব আক্রমণ প্রচেষ্টা	১৭৭

অধ্যায় ২ - হ্যাকিংয়ের পরিকল্পনা



হ্যাকিংয়ের বিভিন্ন ধাপ

যারা হ্যাকার তাদের উদ্দেশ্যই হলো তথ্যনিরাপত্তার তিন মূল ক্ষেত্রের যেকোনো এক বা একাধিক ক্ষেত্র যেভাবেই পারা যায়, আংশিক বা সম্পূর্ণ বিপর্যস্ত করে দেওয়া। তাদের উদ্দেশ্য অবশ্যই অসৎ - সে তথ্য চুরি, আর্থিকভাবে লাভবান হওয়া, কোনো প্রতিষ্ঠানের আইটি সিস্টেমের ক্ষতি করা বা সেই আইটি সম্পদকে অবৈধভাবে অন্য কোনো ক্ষতিকর কাজে ব্যবহার করা। সর্বোপরি, তারা আইনের দৃষ্টিতে অপরাধী। এভাবে যারা অপরাধ করার মানসিকতায় বিনা অনুমতিতে কারো সিস্টেমে অনুপ্রবেশ করে বা করার চেষ্টা করে, তাদেরকে ব্ল্যাক হ্যাট হ্যাকার বলা হয়।

তাহলে এথিক্যাল হ্যাকার (ethical hacker) কারা? এথিক্যাল হ্যাকার বা হোয়াইট হ্যাট (white hat) হ্যাকার হলেন একজন নিরাপত্তা বিশেষজ্ঞ, যিনি একজন ব্ল্যাক হ্যাট হ্যাকারের মতোই তথ্যব্যবস্থা (information system)-কে আক্রমণ করেন; তবে সেটি করার আগে অনুমতি নিয়ে নেন এবং আগে থেকে জানিয়ে পূর্বনির্ধারিত সময়ে টেস্ট করেন। এদের আরেক নাম পেনিন্ট্রেশন

(penetration - কোনো সিস্টেমে গোপনে অনুপ্রবেশ করা) টেস্টার। এখানে মূল পার্থক্য হলো, ব্ল্যাক হ্যাট হ্যাকাররা চায় টার্গেট সিস্টেমের ক্ষতি করতে বা তথ্য ছুরি করতে, অন্যদিকে এথিক্যাল হ্যাকাদের উদ্দেশ্য মহৎ - তারা টার্গেট সিস্টেমের নিরাপত্তা দুর্বলতা চিহ্নিত করে এবং কোন কোন ফাঁকফেক কর বন্ধ করলে হ্যাকারদের অপতৎপরতা ব্যাহত করা যাবে, সেগুলো খুঁজে বের করে নিরসনের পথ বাতলে দেয়। অনেকটা আমাদের বিসিআই এজেন্ট মাসুদ রানার মতো - কাউকে আগ বাড়িয়ে আক্রমণ করা নয়, বরং আক্রান্ত হলে যাতে ঠেকাতে পারি কিংবা আগে থেকে শক্রপক্ষের গুণ্ঠচরদের (এক্ষেত্রে হ্যাকারদের) কুমতলব ধরে ফেলতে পারার মতো প্রস্তুতি আছে কি না সেটি যাচাই করাই আমাদের লক্ষ্য! এই দুই রকম হ্যাকিংয়ের মাঝখানে গ্রে হ্যাট হিসেবে অন্য আরেক দল আছেন, যারা মূলত নিরাপত্তা গবেষক বা ফ্রিল্যান্সার। তারা বিভিন্ন প্রটোকল, অ্যাপ্লিকেশন, অ্যালগরিদম বা টেকনোলজি নিয়ে গবেষণা করে তাদের মাঝে কোনো দুর্বলতা থাকলে সেটি আবিষ্কার করেন এবং সেই দুর্বলতা ব্যবহার করে কীভাবে অনুপ্রবেশ করা যায় তা প্রমাণ (প্রুফ অব কনসেপ্ট) দিয়ে দেখিয়ে দেন। তবে তারা তাদের আবিষ্কারের প্রমাণ জনসমক্ষে প্রকাশের আগেই সেই টেকনোলজি বা অ্যাপ্লিকেশন প্রোভাইডারকে বিস্তারিত জানিয়ে দেন এবং একটা নির্দিষ্ট সময় পর্যন্ত অপেক্ষা করেন, যাতে চাইলে সেই প্রোভাইডার সমস্যাগুলো ঠিক করে ফেলতে পারেন। পাশাপাশি কোনো কোনো ওয়েবসাইট বা অ্যাপ্লিকেশন প্রোভাইডার তাদের দুর্বলতা বা বাগ খুঁজে বের করে প্রমাণসহ জানিয়ে দিলে অনেক সময় সন্ধানদাতাকে পুরুষার দিয়ে কৃতজ্ঞতা স্বীকার করেন।

এথিক্যাল হ্যাকার হিসেবে একটি পেনিট্রেশন টেস্ট করার জন্য বেশ কিছু মেথড আছে। সব মেথডের লক্ষ্য একই হলেও ঠিক কীভাবে টেস্ট করা হবে এবং টেস্ট শুরু করার আগে টেস্টারকে কতটুকু অভ্যন্তরীণ তথ্য জানানো হবে তার ওপর নির্ভর করেই এই ভিন্নতা। এরকম কয়েকটি টেস্টিং মেথড নিয়ে নিচে সংক্ষিপ্ত আলোচনা করা হলো।

বহিরাক্রমণ টেস্ট (External testing) : যেসব আইটি ডিভাইস, সার্ভিস বা অ্যাপ্লিকেশন সরাসরি ইন্টারনেটে সঙ্গে যুক্ত থাকে (যেমন- ইমেইল সার্ভার, ওয়েব সার্ভার, ডিএনএস ইত্যাদি) তাদের ওপরে বাইরের কোনো টিমকে দিয়ে টেস্ট পরিচালনা করা হয়। ইন্টারনেটে থেকে যেসব সিস্টেমে সরাসরি যোগাযোগ করা যায়, সেই সিস্টেমগুলোর সুরক্ষা ব্যবস্থা কেমন, আক্রমণের মুখে সেগুলো কীভাবে ঢিকে থাকতে পারে, হ্যাকার কী কী গোপন তথ্য হাতিয়ে নিতে পারে, কিংবা তখন বিকল্প কোনো উপায়ে সার্ভিস চালু রাখা সম্ভব হবে কি না ইত্যাদি জানার উদ্দেশ্যেই এ ধরনের টেস্ট করা হয়।

অভ্যন্তরীণ টেস্ট (Internal testing) : যেসব ডিভাইস, সার্ভার বা অ্যাপ্লিকেশন সরাসরি ইন্টারনেটের সঙ্গে যুক্ত নয় অথবা ফায়ারওয়াল জাতীয় নিরাপত্তা সিস্টেমের পেছনে থাকে,

সেগুলোর দুর্বলতা পরীক্ষা করাই এই টেস্টের প্রধান উদ্দেশ্য। এক্ষেত্রে টেস্টারকে কিছু নেটওয়ার্ক বা সিস্টেম অ্যাক্সেস প্রদান করা হয়। কোনো হ্যাকার যদি ফিশিং (Phishing) বা অন্য কোনো উপায়ে একটি প্রতিষ্ঠানের কোনো ব্যবহারকারীর আইডি/পাসওয়ার্ড পেয়ে যায়, কিংবা কোনো ম্যালওয়্যার বা রিমোট অ্যাক্সেস টুল (Remote access tool) ইনস্টল করতে সক্ষম হয়, তাহলে সে ওই প্রতিষ্ঠানের কী কী ক্ষতি করতে পারবে, এক্ষেত্রে সেটি জানার চেষ্টা করা হয়।

ব্লাইন্ড বা ব্ল্যাক বক্স টেস্টিং (Blind testing) : ব্লাইন্ড টেস্টিংয়ের ক্ষেত্রে টেস্টারকে কোনো তথ্যই প্রদান করা হয় না। এই পরীক্ষার মূল উদ্দেশ্য হলো কোনো অভ্যন্তরীণ তথ্য জানা না থাকলে একজন হ্যাকার একটি প্রতিষ্ঠানের সিস্টেম সম্পর্কে ইন্টারনেটের মাধ্যমে প্রাপ্ত তথ্য ব্যবহার করে কতদুর অনুপ্রবেশ করতে পারে বা কেমন ক্ষতি করতে পারে, তা জানার চেষ্টা করা। সাধারণত সামরিক বা চরম গোপনীয় সিস্টেমের ক্ষেত্রে এই পদ্ধতি বেশি কার্যকর।

ডাবল ব্লাইন্ড টেস্টিং (Double blind testing) : ব্লাইন্ড টেস্টিংয়ের মতো এক্ষেত্রেও টেস্টারকে কোনো তথ্য জানানো হয় না। একই সঙ্গে অভ্যন্তরীণ নিরাপত্তা টিমকেও আগে থেকে কিছুই জানানো হয় না। এটি করা হয় যাতে বিনা নোটিশে হঠাৎ আক্রমণ হয়ে গেলে ওই প্রতিষ্ঠানের সতর্কীকরণ, প্রতিরক্ষা এবং আক্রমণের মুখে সাড়া দেওয়ার ব্যবস্থা কেমন কাজ করে তা দেখা যায়। অনেক সময় এই আক্রমণকারী টিমকে বলা হয় লাল দল (রেড টিম), যারা যেকোনো উপায়ে অনুপ্রবেশ করা, গোপন তথ্য হাতিয়ে নেওয়া বা সিস্টেম অচল করে দেওয়ার প্রচেষ্টা চালায়। অন্যদিকে অভ্যন্তরীণ প্রতিরক্ষা বা নীল দলের (ব্লু টিম) দায়িত্ব হচ্ছে যত দ্রুত সন্তুষ্ট সেই আক্রমণ ব্যর্থ করে দেওয়া কিংবা ব্যর্থ করতে না পারলেও বিকল্প উপায়ে সিস্টেম চালু রাখা। এতে করে বাস্তব জীবনে বড়ো আক্রমণ হলে প্রতিরক্ষা ব্যবস্থা কী কী সমস্যার সমুখীন হতে পারে সে সম্পর্কে সত্যিকারের ধারণা নিয়ে সেগুলোর সমাধান খুঁজে বের করা যায়।

বিশেষ পরিস্থিতি যাচাই (Targeted simulation) : এক্ষেত্রে টেস্টার এবং অভ্যন্তরীণ নিরাপত্তা টিম দুই পক্ষ একসঙ্গে কাজ করে। টেস্টার কীভাবে আক্রমণ করছে সেটি জেনে তদারকি (monitoring), সতর্কীকরণ (detection) ও প্রতিরক্ষা ব্যবস্থা কেমন সাড়া (incident respons) দিচ্ছে, বা আক্রমণ ঠেকাতে পারছে না কেন সেটি যৌথভাবে বিশ্লেষণ করে দেখা হয়। এর ফলাফল হিসেবে নিরাপত্তাব্যবস্থা জোরদার করার কর্মসূচি গ্রহণ করা হয়।

গ্রে বক্স টেস্টিং (Grey box testing) : সীমিত সময়সীমার মধ্যে ভালো ফলাফল পেতে বাস্তবে মাঝামাঝি একটি মডেল অনুসরণ করা হয়। এতে একদম কিছু না জেনে টেস্ট শুরু করা হয় না, আবার সবকিছু যে জানিয়ে দেওয়া হয়, তাও না। এক্ষেত্রে এথিক্যাল হ্যাকারকে ইন্টারনেটে যুক্ত সিস্টেম সম্পর্কে মোটামুটি তথ্য দেওয়া হয়। আর সেই সঙ্গে অভ্যন্তরীণ নেটওয়ার্কে কী কী

সফটওয়্যার ব্যবহার করা হয় এবং ব্যবহারকারীদের ধরন সম্পর্কে প্রাথমিক ধারণা দেওয়া হয়। অভ্যন্তরীণ ঝুঁকি যাচাই করার জন্য সাধারণ ব্যবহারকারী (End user) বা গ্রাহকের অ্যাকসেস সংবলিত সীমিত ক্ষমতার ইউজার আইডি দিয়ে দেওয়া হয়। বাইরের কোনো হ্যাকারের কাছে সাধারণ ব্যবহারকারীর আইডি-পাসওয়ার্ড অথবা ম্যালওয়ারের মাধ্যমে কিছু না কিছু অভ্যন্তরীণ সিস্টেম অ্যাকসেস থাকতে পারে, এমনটি ধরে নিয়ে সেরকম পরিস্থিতিতে সে কী কী ক্ষতি করতে পারে তা জানাই এই মডেলের উদ্দেশ্য।

বিভিন্ন প্রতিষ্ঠান এভাবে এথিক্যাল হ্যাকারদের সাহায্য নিয়ে টেস্টের ফলাফল দেখে প্রতিনিয়ত নিজেদের তথ্যনিরাপত্তা-ব্যবস্থা উন্নত করতে সচেষ্ট। আইটি সেক্টরের ক্রমবর্ধমান কর্মসূচি সারা বিশ্বেই তাই এদের চাহিদা ব্যাপক! এই বইয়ের মাধ্যমে হ্যাকারদের অপতৎপরতার বিরুদ্ধে আমরা সাইবার জগতের দায়িত্বশীল কাউন্টার এজন্ট মাসুদ রানা (!) হতে গেলে কী কী বিষয় জানা দরকার এবং কোন টুল কীভাবে ব্যবহার করতে হবে, সেটি শেখার চেষ্টা করব। তবে সিনেমায় যেভাবে দেখানো হয় যে হ্যাকাররা দুই মিনিটের মধ্যে যেকোনো সিস্টেমে অনুপ্রবেশ করে ফেলে, বাস্তবে ব্যাপারটা মোটেও এত নাটকীয় নয়। যেকোনো সফল হ্যাকিংয়ের জন্য বহুদিন ধরে টাগেট সিস্টেম সম্পর্কে তথ্য সংগ্রহ করে, তারপর সেগুলো বিশ্লেষণ করে ধাপে ধাপে বিভিন্ন দুর্বলতা চিহ্নিত করে, কোন লক্ষ্যবস্তুতে কীভাবে আক্রমণ করা যায় তার জন্য বিশাল প্রস্তুতি গ্রহণ করা হয়। সব মিলিয়ে শুরু থেকে শেষ পর্যন্ত একটি পূর্ণাঙ্গ এথিক্যাল হ্যাকিং বা পেনিট্রেশন টেস্টিং প্রকল্পকে মোটামুটি চার ভাগে ভাগ করা যায় :

1. প্রস্তুতি (Planning)

- a. কর্মপরিধি (Pre-Engagement)
- b. তথ্য সংগ্রহ (Reconnaissance)

2. আক্রমণ কৌশল (Analysis)

- a. ঝুঁকি চিহ্নিতকরণ (Scanning)
- b. দুর্বলতা বিশ্লেষণ (vulnerability assessment)

3. পেনিট্রেশন (Penetration)

- a. অনুপ্রবেশ (Exploitation)
- b. নিয়ন্ত্রণ (Post Exploitation)

4. সমাপ্তি (Closing)

- a. প্রতিবেদন (Reporting)
- b. পুনঃপরীক্ষা (Validation and Re-Testing)

কর্মপরিধি (Engagement scope)

আমরা যেহেতু এথিক্যাল হ্যাকার, তাই অবশ্যই যথাযথ কর্তৃপক্ষের পূর্বানুমতি নিয়ে কাজটি শুরু করব। তবে 'সবকিছু টেস্ট করে দেখুন' এভাবে আসলে কোনো কিছু শুরু করা যায় না। প্রথমে আমাদেরকে জানতে হবে যে কোন কোন সিস্টেম টেস্ট করতে হবে। পুরো প্রতিষ্ঠানের সবকিছু একবারে অল্প সময়ে টেস্ট করা হয়তো সম্ভব নয়, তার দরকারও নেই। কোনো প্রতিষ্ঠানের গুরুত্বপূর্ণ সিস্টেমগুলো কী কী তা চিহ্নিত করা ওই প্রতিষ্ঠানের অভ্যন্তরীণ নিরাপত্তা টিমের দায়িত্ব। সেই গুরুত্বপূর্ণ সিস্টেমের তালিকা পরীক্ষা করে আমাদেরকে বুঝতে হবে কোনগুলো সরাসরি ইন্টারনেটের সঙ্গে যুক্ত আর কোন কোন সিস্টেমে অনুপ্রবেশ করার অনুমতি দেওয়া হলো। সেই সঙ্গে টেস্টের সময় কী কী করা যাবে বা কী করা যাবে না (যেমন- সিস্টেম অচল করে দেওয়া বা কোনো গোপনীয় তথ্য পরিবর্তন করা যাবে না) তা বুঝে নেওয়া। সব মিলিয়ে কতদিন ধরে টেস্ট করা যাবে, টেস্টের ধরন, টার্গেট সিস্টেম ও অ্যাপ্লিকেশনের তালিকা, টেস্ট ইউজার, আইপি রেজ্ঞ, কোন সিস্টেমে কী ধরনের টেস্ট করা যাবে ইত্যাদি পয়েন্ট নিয়ে আলোচনা করে পুরো বিষয়টির লিখিত রূপ তথ্য কর্মপরিধি (Scope) তৈরি করে তাতে প্রতিষ্ঠানের অনুমোদন নিতে হবে।

তথ্য সংগ্রহ (Reconnaissance)

এথিক্যাল হ্যাকিংয়ের কর্মপরিধি অনুমোদিত হওয়ার পরে প্রথম যে কাজটি করতে হবে তা হলো : ওই প্রতিষ্ঠানের পুরো আইটি সিস্টেম সম্পর্কে সম্পর্কে সম্পর্কে ধারণা নেওয়া। প্রতিষ্ঠানের কাছ থেকে পাওয়া তথ্যের পাশাপাশি নিজস্ব প্রয়াসে ইন্টারনেট বা অন্যান্য উৎস থেকে যত বেশি সম্ভব তথ্য জোগাড় করতে হবে। যেহেতু এথিক্যাল হ্যাকারের জন্য নির্দিষ্ট সময়সীমা বেঁধে দেওয়া থাকে, সেহেতু প্রথমেই সবচেয়ে ঝুঁকিপূর্ণ বা বেশি দুর্বল লক্ষ্যবস্তুকে আক্রমণের টার্গেট করাই বুদ্ধিমানের কাজ। তারপর সময় থাকলে অন্যান্য লক্ষ্যবস্তুতে আক্রমণের চেষ্টা করা যেতে পারে। সেজন্য প্রথমেই নেটওয়ার্কের ভেতরে কোন কোন প্রটোকল চলে, কোন পোর্টে কী সার্ভিস চালু আছে, ডিভাইসের ফার্মওয়ারের ভার্শন কত, কোন অপারেটিং সিস্টেম বা কোন অ্যাপ্লিকেশন ব্যবহার করে সার্ভিস দিচ্ছে ইত্যাদি বিস্তারিত তথ্য বের করে ফেলা দরকার।

ঝুঁকি চিহ্নিতকরণ (Scanning)

নানাভাবে প্রাপ্ত তথ্য ব্যবহার করে টার্গেট নেটওয়ার্ক এবং ওয়েব অ্যাপ্লিকেশন আর্কিটেকচারের একটি রূপরেখা দাঁড় করানো হয়। তারপর স্ক্যানিং টুল চালিয়ে কোন সার্ভিস বা পোর্ট চালু আছে এবং সেগুলোতে কোনো দুর্বলতা আছে কি না, তা যাচাই করা হয়। কোন সফটওয়্যারের ভেতর কী কী দুর্বলতা আছে তা জানার জন্য বহুল প্রচলিত উৎস হচ্ছে সিভিই (Common

Vulnerabilities and Exposures)। বিশেষ করে, <https://cve.mitre.org/> বা <https://nvd.nist.gov/> এই দুই ওয়েবসাইট ঘাঁটাঘাঁটি করে জানা যায় যে, কোন সফটওয়্যারের কোন ভার্ষনে কী কী দুর্বলতা আছে এবং দুর্বলতা থাকলে তার ঝুঁকির মাত্রা কত (0-9) জানা যায়। হ্যাকাররা এই দুর্বলতার বিষয়ে সংশ্লিষ্ট ভেন্ডরের বক্তব্য (security advisory বা Knowledge Base) থেকে সিস্টেমের দুর্বল পয়েন্টগুলো বুঝতে চেষ্টা করে।

প্রতিটি সফটওয়্যার প্রস্তুতকারক তাদের ওয়েবসাইটে নিরাপত্তাক্রতি নিয়ে বিস্তারিত তথ্য (Knowledge base) আর তা নিরসনের উপায় (Security advisory) বলে দেয়। প্রতিটি ক্রটি প্রকাশিত হওয়ামাত্রাই সেটিকে একটি সিভিই নম্বর দেওয়া হয়, যা ব্যবহার করে গুগলে খুঁজলেই অনেক তথ্য পাওয়া যায়। হ্যাকাররা এসব নিরাপত্তা ক্রটির বিস্তারিত তথ্য পর্যালোচনা করে খুব তাড়াতাড়ি আক্রমণের উপায় (proof of concept) বের করে ফেলে। উল্লেখ্য যে, যেসব নিরাপত্তা ক্রটি সদ্য আবিষ্কৃত হয়েছে, কিন্তু এখনো যার নিরসন (bug fix) বা প্যাচ (security patch) রিলিজ হয়নি, সেগুলোকে জিরো ডে (Zero day) দুর্বলতা বলে।

আজকাল অবশ্য ঝুঁকি চিহ্নিতকরণের কাজটুকু ম্যানুয়ালি না করে অটোমেটিক স্ক্যানিং টুল ব্যবহার করেই করা হয়। তারপর টুল থেকে পাওয়া ফলাফল বিশ্লেষণ করে ওই প্রতিষ্ঠানের কার্যক্রম, কাস্টমার বা ব্যাবসায়িক পরিমণ্ডল আর আর্কিটেকচার বিবেচনা করে কোন কোন দুর্বলতা আসলেই সেই প্রতিষ্ঠানের জন্য বেশি বিপজ্জনক বা বড়োসড়ো ক্ষতির কারণ হতে পারে তা নির্ধারণ করা হয়। এই প্রক্রিয়াকে বলা হয় ঝুঁকি নির্ণয় (Risk assessment)। সিভিই স্কোর সবার জন্য এক হলেও এই নিজস্ব ঝুঁকির মাত্রা প্রতিষ্ঠানভেদে আলাদা হয়। যেমন- যে প্রতিষ্ঠানে মোবাইল অ্যাপে লোকাল ডেটা সংরক্ষণ করা হয় না, তাদের জন্য একটি মোবাইল ডিভাইসের এনক্রিপশন দুর্বলতা (সিভিই স্কোর 8+ হলেও) হয়তো তেমন ক্ষতিকর নয়।

যাচাই করে নিন (Test your knowledge)

Secure Socket Layer (SSL) প্রটোকলভিত্তিক ডিজিটাল সার্টিফিকেট এক সময় বিভিন্ন ওয়েবসাইটে ব্যাপকভাবে ব্যবহৃত হতো। কিন্তু গত কয়েক বছরে এর বিভিন্ন ভার্ষনে নানা রকম দুর্বলতা (যেমন- পুড়ল, হার্টব্লিড) আবিষ্কৃত হয়েছে, যা ব্যবহার করে গুপ্ত বার্তার পাঠোদ্ধার করা যায়। একটু ইন্টারনেট ঘেঁটে দেখ নিন না এই দুর্বলতার উৎস, সম্ভাব্য ক্ষতির মাত্রা আর তার সিভিই স্কোর কত?

দুর্বলতা বিশ্লেষণ (Vulnerability assessment)

প্র্যানিং টুলগুলোর ফলাফল বিশ্লেষণ করে তার সঙ্গে ওই প্রতিষ্ঠানের অন্যান্য তথ্য মিলিয়ে একজন একিক্যাল হ্যাকার বুকাতে পারেন কোন দুর্বলতা ব্যবহার করে অনুপ্রবেশের চেষ্টা করলে সফল হওয়ার সম্ভাবনা সবচেয়ে বেশি। সেই সঙ্গে কোন দুর্বলতা ব্যবহার করলে কী টুল বা কী উপায় অবলম্বন করতে হবে, কী রকম সময় লাগতে পারে, কোন সিস্টেমের সুরক্ষা ভেদ করা বেশি গুরুত্বপূর্ণ ইত্যাদি বিয়য়ের ওপর ভিত্তি করেই তার আক্রমণ পরিকল্পনা চূড়ান্ত করেন। চিহ্নিত দুর্বলতা ব্যবহার করে অনুপ্রবেশ করা সম্ভব কি না, সেটি সিভিই ক্ষেত্র, পাবলিক এঞ্জিনিয়ের (অর্থাৎ, ইন্টারনেটে সহজেলভ্য টুল আছে কি না), হ্যাকিংয়ের শিকার হয়ে গেলে ক্ষতির পরিমাণ কত হতে পারে, ইত্যাদি যাচাই করে যুক্তিসংগত অনুমান করে নেওয়া হয়।

এঙ্গের উল্লেখ্য যে, অনেক প্রতিষ্ঠানে এই ধাপের পরপরই কী কী দুর্বলতা আছে এবং তার মধ্যে কোনগুলো সবচেয়ে বেশি ঝুঁকিপূর্ণ তা জানতে চায়। অনুপ্রবেশ করার প্রমাণের অপেক্ষায় না থেকে, বেশি ঝুঁকিপূর্ণ সফটওয়্যারকে আপডেট করে বা কনফিগারেশন পরিবর্তন করে সহজেই সুরক্ষার মাত্রা অনেকগুণে বাড়ানো সম্ভব। বিশেষ করে নিয়মিত অভ্যন্তরীণ টেস্টের ক্ষেত্রে মূলত দুর্বলতা বিশ্লেষণ প্রতিবেদন (vulnerability assessment report) দেখেই কাজ করা হয়।

সত্যি সত্যি অনুপ্রবেশ করে একাধিক ঝুঁকিপূর্ণ সিস্টেমের নেওয়া বেশ সময়সাপেক্ষ ব্যাপার, আবার প্রোডাকশন সিস্টেমে আক্রমণ করে পেনিট্রেশন টেস্ট করার চেষ্টা সব সময় পুরোপুরি নিরাপদ নাও হতে পারে। যেহেতু প্রতি সপ্তাহে বা প্রতি মাসে নিয়মিত বিস্তৃত আকারে (Comprehensive) পেনিট্রেশন টেস্ট করা সম্ভব নয়, তাই সাধারণত বছরে একবার করে পূর্ণাঙ্গ এঞ্জিনিয়ের পেনিট্রেশন টেস্ট করা হয়। অন্য সময় সব সিস্টেম নিয়মিত ক্ষ্যান করে ঝুঁকি নির্ণয়ের পাশাপাশি অধিক ঝুঁকিপূর্ণ ক্ষেত্রে সীমিত আকারে কিছু অভ্যন্তরীণ ম্যানুয়াল পেনিট্রেশন টেস্ট করা হয়।

অনুপ্রবেশ ও নিয়ন্ত্রণ (Exploitation and post-exploitation)

কোনো প্রতিষ্ঠানের প্রতিরক্ষা ব্যবস্থা ভেদ করে সফলভাবে একটি সিস্টেমে অ্যাক্সেস (যেখানে টেস্ট অ্যাকাউন্ট ব্যবহার করে চুক্তে পারার কথা না) করতে সক্ষম হলে তাকে অনুপ্রবেশ (Exploitation) বলা যায়। সাধারণত দুর্বলতা বিশ্লেষণ পর্যায়ে চিহ্নিত করা বেশি ঝুঁকিপূর্ণ সিস্টেম বা অ্যাপ্লিকেশনের ওপর পূর্বপরিকল্পিত আক্রমণ চালিয়ে অনুপ্রবেশের চেষ্টা করা হয়। সেই অ্যাপ্লিকেশন বা সিস্টেম প্রস্তুতকারক প্রতিষ্ঠান আগে থেকেই তাদের এসব দুর্বলতা সম্পর্কে ইন্টারনেটে তথ্য দিয়েছে যার ভিত্তিতে অনেক নিরাপত্তা গবেষক কোড লিখে (শেল বা পাইথন দিয়ে) এই দুর্বলতা ব্যবহার করে কীভাবে অনুপ্রবেশ করা যায় তার বাস্তব প্রমাণ (Proof of

concept) হাজির করেছেন। প্রচলিত টুলগুলো এসব প্রুফ অফ কনসেপ্টের ভিত্তিতে তাদের ফিচার বা মডিউল নিয়মিত আপডেট করে নেয়। চাইলে আপনি নিজেও সরাসরি স্ক্রিপ্ট লিখে আক্রমণ করতে পারেন। তবে আমরা যেহেতু সবেমাত্র এথিক্যাল হ্যাকার হওয়ার দিকে যাত্রা শুরু করেছি, তাই অনুপ্রবেশ করার জন্য বরং যেসব উন্মুক্ত বা সহজলভ্য টুল পাওয়া যায় সেগুলোই আগে শিখব।

কোনো সিস্টেমে সফলভাবে অনুপ্রবেশের পর হ্যাকার তার নিয়ন্ত্রণ গ্রহণ (Post Exploitation) করতে চায়। একজন হ্যাকার সিস্টেম চুক্তে গেছে তার মানে এই নয় যে সে তখন যা খুশি তা-ই করতে পারে। অনেক ক্ষেত্রে কোনো একটি সিস্টেমে অনুপ্রবেশ করা সম্ভব হলেও আগে থেকে ইনস্টল করা অন্যান্য নিরাপত্তাব্যবস্থার কারণে ওই সিস্টেম থেকে গোপন তথ্য বের করা বা কিছু কিছু কমান্ড রান করা সম্ভব হয় না। চাইলেই সাধারণ অ্যাকাউন্ট থেকে অ্যাকসেস করে শক্তিশালী অনেক কমান্ড (Privileged access command) রান করা সম্ভব হয় না। তাই এক্ষেত্রে খুব সাবধানে এগোতে হয়, তা না হলে যেকোনো সন্দেহজনক কার্যক্রম চট করে নিরাপত্তা সতর্কীকরণ ব্যবস্থার আওতায় ধরা পড়ে অ্যাকাউন্ট বা অ্যাকসেস পোর্ট ব্লক হয়ে যেতে পারে। তাই এই পর্যায়ে ধরা না পড়ে কীভাবে তথ্য সংগ্রহ বা নিয়ন্ত্রণ গ্রহণ করা যায়, সেটিই মুখ্য উদ্দেশ্য থাকে।

হ্যাকাররা চেষ্টা করে অনুপ্রবেশকৃত ওই সিস্টেমে বা ডিভাইসে কোনো রকম ম্যালওয়্যার বা রিমোট অ্যাকসেস টুল (RAT - Remote access tool) কিংবা বট (Bot - যা দিয়ে দূর থেকে নির্দেশনা পাঠিয়ে হোস্ট ডিভাইসকে গোপনে অন্য কাজে ব্যবহার করা যায়) ইনস্টল করা যায় কি না, গেলে তো কেল্লা ফতে! তখন রিমোট সিস্টেম থেকে এই ম্যালওয়্যার দিয়ে টার্গেট হোস্টে বিভিন্ন কমান্ড রান করা যায়, কনফিগারেশন এডিট করা যায় অথবা একই নেটওয়ার্কের অন্য সিস্টেমে প্রবেশ করা যায়। এভাবে একসঙ্গে অসংখ্য হোস্টে বট ইনস্টল করতে পারলে পরবর্তীতে হাজার হাজার বট ব্যবহার করে অন্য আরেকটি প্রতিষ্ঠানকে হঠাতে আক্রমণ করে বিশাল ট্রাফিক পাঠিয়ে দিয়ে তাদের সিস্টেম বা নেটওয়ার্ক অচল করে দেওয়ার (DDoS - Distributed Denial of Service Attack) চেষ্টা করা যায়।

প্রমাণ নিশ্চিহ্নকরণ (Clearing Tracks)

এটি মোটেও কোনো এথিক্যাল হ্যাকারের কাজ নয়। তবে আসল হ্যাকার কোনো একটি সিস্টেমে অনুপ্রবেশ করে সে যেসব অবৈধ কাজ করেছিল অনেক সময় সেই চিহ্নগুলো বা লগ মুছে দেওয়ার চেষ্টা করে, যাতে পরবর্তীতে কেউ তার হ্যাকিংয়ের প্রমাণ খুঁজে বের করতে না পারে। হ্যাকারের অনুপ্রবেশ প্রচেষ্টার তদন্ত, তাদের কর্মকাণ্ডের সূত্র খোঁজা এবং দালিলিক প্রমাণ উদ্বার করার জন্য

আলাদা কিছু কার্যপদ্ধতি আছে। এটি তথ্যনিরাপত্তার অন্য একটি শাখা যা হ্যাকিং প্রমাণ অনুসন্ধান (Hacking Forensic) নামে বিশেষ পরিচিত।

প্রতিবেদন উপস্থাপন (Reporting)

এখিক্যাল হ্যাকার হিসেবে বিভিন্ন দুর্বলতা বিশ্লেষণ করে বিশেষ কিছু ঝুঁকি চিহ্নিত করে ওই প্রতিষ্ঠানের বিভিন্ন সিস্টেমে অনুপ্রবেশ করে বা নিয়ন্ত্রণ গ্রহণ করে কী কী ক্ষতি করা সম্ভব, পেনিট্রেশন টেস্ট শেষ করে তার ফলাফল সুন্দরভাবে লিখিত প্রতিবেদন (Penetration test report) আকারে উপস্থাপন করতে হবে। এই প্রতিবেদন এমনভাবে লিখিতে হবে, যাতে প্রতিষ্ঠানের ব্যবস্থাপনা কর্তৃপক্ষ তাদের নিরাপত্তাব্যবস্থার ঝুঁকি বা দুর্বলতাগুলো সঠিকভাবে বুঝতে সক্ষম হন। সেখানে কোনটি বেশি ঝুঁকিপূর্ণ বা কোনটি কম তার যুক্তিগ্রাহ্য ব্যাখ্যা দিতে হবে আর সেই ঝুঁকি রোধ করার জন্য কী রকম পদক্ষেপ নেওয়া যেতে পারে, তার সুপারিশ করতে হবে।

যাচাই ও পুনঃপরীক্ষা (Validation and Re-testing)

প্রাথমিক প্রতিবেদন পাওয়ার পর টেস্টিং টিমের প্রধান বা সিনিয়র রিভিউয়ার প্রতিটি ফল যাচাই (validation) করে দেখেন। যেকোনো টুলই কিছু কিছু ক্ষেত্রে ফলস পজিটিভ (আপাতদৃষ্টিতে দুর্বলতা মনে হলেও, সেটি সঠিক নয়) ফল দিতে পারে। আবার অনেক সময় ওই প্রতিষ্ঠান যেভাবে সার্ভিস দেয় বা যেভাবে কাজ করে, তার পরিপ্রেক্ষিতে হয়তো সংশ্লিষ্ট দুর্বলতা অপ্রাসঙ্গিক বা তেমন ক্ষতিকর নয়। তাই প্রাপ্ত ফলাফলের ওপর যাতে ওই প্রতিষ্ঠানের আইটি বা সফটওয়্যার বিভাগ দ্বিমত পোষণ করতে না পারে, তা ভালোভাবে যাচাই করে এবং প্রামাণ্য নমুনা যুক্ত করে চূড়ান্ত প্রতিবেদন তৈরি করা হয়।

অতঃপর, প্রতিবেদনে উল্লিখিত দুর্বলতা ঠিক করার জন্য প্রতিষ্ঠানের পক্ষ থেকে অ্যাপ্লিকেশনের ফিচার পরিবর্তন, প্যাচ আপডেট, ভার্শন আপগ্রেড, কনফিগারেশন পরিবর্তন, অদরকারি সার্ভিস বন্ধ, অন্যান্য নিরাপত্তা উন্নয়ন ইত্যাদি অনেক পদক্ষেপ নেওয়া হয়। এসব পদক্ষেপের ফলে প্রাপ্ত সব দুর্বলতা আসলেই নিরসন হয়েছে কি না, সেটি যাচাই করে দেখার জন্য কিছুদিন পর সীমিত আকারে পুনঃপরীক্ষা (retest) করা হয়।

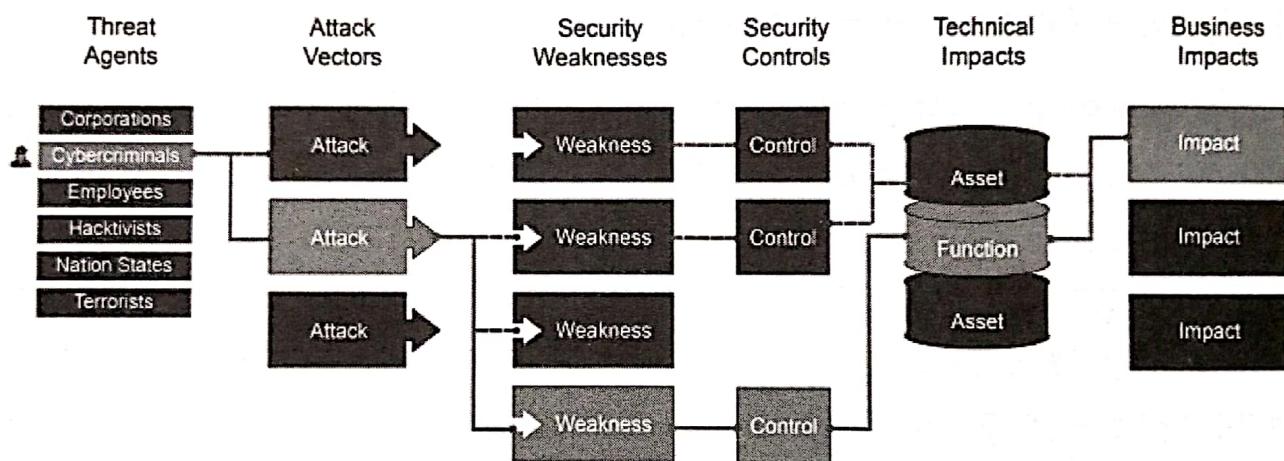
সারসংক্ষেপ

কোন প্রতিষ্ঠান থেকে তাদের সিস্টেমে পেনিট্রেশন টেস্ট করার অনুরোধ পেলে একজন এখিক্যাল হ্যাকার হিসেবে কীভাবে পরিকল্পনা করতে হবে এবং কী কী ধাপ অনুসরণ করে টেস্ট শেষ করে চূড়ান্ত প্রতিবেদন জমা দিতে হবে তার ধারণা পেলাম। টেস্ট শুরুর আগে প্রতিষ্ঠানের ঝুঁকির মাত্রা

এবং প্রয়োজনীয়তা অনুযায়ী কোন ধরনের টেস্ট করতে হবে তা ঠিক করে নিয়ে লিখিত অনুমোদন নিয়ে নিতে হবে। কারণ টেস্টের সময় যা যা করবেন তার সবকিছুই এই পরিসীমার ভেতরে থাকতে হবে, অন্যথায় অনাকাঙ্ক্ষিত দুঃটিনা ঘটলে তার দায়ভার আমাদেরকেই বহন করতে হবে। মনে রাখতে হবে, আমাদের মূল দায়িত্ব অহেতুক কৌতুহল প্রদর্শন নয়, বরং একটি প্রতিষ্ঠানের নির্ধারিত কর্মপরিধির ভেতরে তাদের মাধ্যমে নির্ধারিত টার্গেট সিস্টেমে কী কী ঝুঁকি আছে, তা চিহ্নিত করাই আমাদের একমাত্র লক্ষ্য।

যাচাই করে নিন (Test your knowledge)

নিজের চিত্রকল্প ব্যবহার করে ভাবুন : একটি প্রচলিত ইকমার্স ওয়েবসাইটের প্রধান পাঁচটি নিরাপত্তাঝুঁকি কী কী? আর এই সাইট হ্যাক করতে পারলে হ্যাকারদের কী লাভ হবে এবং প্রতিষ্ঠানের কী কী ক্ষতি হতে পারে?



ছবি 2.1

এভাবে ভাবতে পারলে দেখবেন হ্যাকার আর প্রতিষ্ঠানের লাভ-ক্ষতির দৃষ্টিভঙ্গি কেমন আলাদা!

নৈতিক বিধিনিষেধ

আমাদের উদ্দেশ্য যেহেতু বৈধভাবে দুর্বলতা চিহ্নিত করে হ্যাকারদের অনুপ্রবেশ ঠেকানোর ব্যবস্থা গ্রহণ সাহায্য করা, সেজন্য আমরা চাইলেই যেকোনো সাইট বা সিস্টেমে পেনিট্রেশন করতে পারি না। যেকোনো সিস্টেমে পেনিট্রেশন টেস্ট চালানোর আগে অবশ্যই মালিকপক্ষের লিখিত অনুমতি নিতে হবে। বিনা অনুমতিতে পেনিট্রেশন টেস্ট পরিচালনা করা আইনত দণ্ডনীয় অপরাধ হিসেবে দেখা হয়, সেই সঙ্গে মনে রাখতে হবে আমাদের নৈতিক দায়বদ্ধতাই ব্ল্যাক হ্যাট অপরাধীদের সঙ্গে

এক মৌলিক পার্থক্য গড়ে দেয়। একই কারণে যারা ওয়েব নিরাপত্তা নিয়ে গবেষণা করেন, তারা কোথাও কোনো নিরাপত্তা ত্রুটি আবিষ্কার করলে সাধারণত সবার আগে সেই সিস্টেম, ডিভাইস বা অ্যাপ্লিকেশন নির্মাতাকে জানিয়ে দেন, তারপর যথাসময়ে প্রমাণ (proof of concept) জনসমক্ষে প্রদর্শন করেন। এই পুরো ব্যাপারটির ক্ষেত্রে ‘রিসপনসিবল ডিসঙ্গেজার’ নীতি অনুসরণ করে করা হয়, যার বিস্তারিত জানা যাবে নিচের লিংক থেকে :

<https://iamthecavalry.org/about/disclosure/disclosure-programs/>

নেতৃত্ব বজায় রেখে পেনিট্রেশন টেস্ট পরিচালনা করার ক্ষেত্রে নিচের বিষয়গুলো খেয়াল রাখা খুবই জরুরি :

- নির্ধারিত কর্মপরিধি বা ক্ষেপের বাইরে কোনো ডিভাইস, সিস্টেম বা অ্যাপ্লিকেশনের ওপর পেনিট্রেশন টেস্ট, তথ্য সংগ্রহ কিংবা ক্ষ্যানিং করা একদম উচিত নয়।
- যেকোনো টুল চালনা করার আগে টার্গেট আইপি অ্যাড্রেস এবং সেই ডিভাইস/সিস্টেম ইনফরমেশন ভালোভাবে যাচাই করে সেটি আমাদের অনুমোদিত কর্মপরিধির মধ্যে পড়ে কি না নিশ্চিত হয়ে নিতে হবে।
- গ্রাহকের অ্যাপ্লিকেশন এবং সার্ভিসের ব্যবহারবিধি বুঝে পরিকল্পনা করতে হবে। প্রোডাকশন বা লাইভ এনভায়রনমেন্ট অর্থাৎ আসল ব্যবহারকারীরা যেসব সার্ভার ব্যবহার করে থাকেন, সেখানে পেনিট্রেশন টেস্ট চালাতে গেলে আগে থেকে অনুমতি নিতে হবে।
- আলাদাভাবে বলা না থাকলে, পেনিট্রেশন টেস্টের জন্য প্রোডাকশন, তথা যে সার্ভারের ওয়েব অ্যাপ্লিকেশন সরাসরি গ্রাহকেরা ব্যবহার করেন বা তাদের তথ্য থাকে সেটা নয়, বরং অন্য কোনো ব্যাকআপ সার্ভারে তার ক্লোন এনভায়রনমেন্ট তৈরি করতে অনুরোধ জানিয়ে টেস্টের জন্য সেটি ব্যবহার করাই উত্তম।
- কবে, কখন বা কোন কোন সময় এবং কোন কোন মেশিন বা আইপি অ্যাড্রেস থেকে পেনিট্রেশন টেস্ট চালানো হবে তা আগে থেকে জানিয়ে দিতে হবে, যাতে করে তাদের পক্ষ থেকে কোনটি টেস্টারের কাজ, আর কোনটি অবৈধ কার্যকলাপ, তা চিহ্নিত করতে কোনো অসুবিধা না হয়।
- আলাদাভাবে উল্লেখ করা না থাকলে অনুপ্রবেশ পর্যন্তই টেস্টের সীমারেখা, অর্থাৎ অনুপ্রবেশ করার পর ডেটাবেজ বা সার্ভারে চুকে ইচ্ছেমতো পোস্ট-এন্ডপ্লয়েট কমান্ড চালানো যাবে না। মনে রাখবেন, আমরা গ্রাহকের সিস্টেম আর তথ্যের গোপনীয়তা বজায় রাখতে পূর্বপ্রতিশ্রুতিবদ্ধ।
- আলাদাভাবে বলা না থাকলে তাদের সিস্টেম অচল করে দেওয়ার মতো কোনো টেস্ট করা যাবে না। ক্ষ্যানিং করে সেরকম ত্রুটি পাওয়া গেলে তা রিপোর্টে উল্লেখ করলেই চলবে।

- অনুপ্রবেশের প্রমাণ হিসেবে সিস্টেম এন্সেসের ক্রিনশট বা ‘রিড বা ভিউ অনলি’ কমান্ড চালিয়ে তার ফলাফল দেখানোই যথেষ্ট। কখনোই তাদের ডেটাবেজে সংরক্ষিত কোনো রকম তথ্য বা সার্ভার কনফিগারেশন পরিবর্তন করা যাবে না।
- স্ক্যানিং থেকে শুরু করে পরবর্তী প্রতিটি পদক্ষেপের রেকর্ড এবং টুলের লগ সংরক্ষণ করতে হবে।

পরোক্ষ তথ্য সংগ্রহ

এক অর্থে হ্যাকিং হলো বিশাল জটিল কিছু ধাঁধার চমকপ্রদ সমাধান, তবে সেই সমাধান বাঁকা পথে বের করা। এথিক্যাল হ্যাকিং হলো এই বাঁকা পথে সমাধান খোঁজার ইতিবাচক প্রয়াস অর্থাৎ বাঁকা পথ খুঁজে বের করে তা বন্ধ করতে সাহায্য করা। নিরাপত্তা দুর্বলতা আবিষ্কারের কোন নির্দিষ্ট ফরমুলা নেই, সিস্টেম কনফিগারেশন অনুযায়ী বিভিন্ন উপায় অবলম্বন করে তা বের করা সম্ভব। এথিক্যাল হ্যাকিংয়ের চিন্তাকর্ষক যাত্রার শুরুতে কোন রাস্তা ধরে হ্যাকিং করতে হবে বা সিস্টেমে অনুপ্রবেশ করা যাবে তা ঠিক করা এক গুরুত্বপূর্ণ পদক্ষেপ। তাই টার্গেট সিস্টেমে সম্পর্কে বিস্তারিত জানার জন্য অনেকটা দুর্দান্ত গোয়েন্দার মতো প্রত্যক্ষ এবং পরোক্ষ দুই রকম উপায়েই প্রচুর তথ্য সংগ্রহ (reconnaissance) করতে হয়।

টার্গেট সিস্টেমের সঙ্গে সরাসরি কোনো যোগাযোগ (network communication or interaction) না করে মূলত ইন্টারনেটে প্রাপ্ত উন্মুক্ত উৎস (public information) ব্যবহার করে পরোক্ষভাবে তথ্য জোগাড় (Passive reconnaissance) করা হয়। অন্যদিকে টার্গেট সিস্টেমে নেটওয়ার্ক প্রটোকল দিয়ে বার্তা পাঠিয়ে তার সাড়া ঘাচাই করে প্রত্যক্ষভাবে তথ্য জোগাড় (Active reconnaissance) করা হয়।

অনেক সময় এই অনুসন্ধান থেকে চমকপ্রদ অর্থচ একদম অপ্রত্যাশিত কিছু তথ্য হাতে চলে আসতে পারে। দেখা গেল, অনেক অনিরাপদ ডিভাইস ইন্টারনেটে যুক্ত থাকারই কথা নয়, তবু তা যুক্ত আছে – যা সহজেই অনুপ্রবেশের রাস্তা খুলে দিতে পারে। তেমনি কর্মীদের অভ্যন্তরীণ আইডি, ইমেইল অ্যাড্রেস বা ফাঁস হয়ে যাওয়া পাসওয়ার্ড হাতে চলে আসা অসম্ভব নয়। কীভাবে বা কোন টুল ব্যবহার করে এই পরোক্ষ তথ্য সংগ্রহের কাজটি করা হয়, আমরা এবারে তা বিস্তারিত দেখব।

Whois

Whois হলো সবার জন্য উন্মুক্ত একটি ডেটাবেজ, যেখানে যেকোনো ওয়েবসাইট অ্যাড্রেস বা ভোমেইনের মালিকানা, যোগাযোগের ঠিকানা, নেম সার্ভার, হোস্টিং আইপি অ্যাড্রেস ইত্যাদি তথ্য থাকে। ইন্টারনেটে অনেক ওয়েবসাইট আছে যেখানে ভ-ইজ বিষয়ক তথ্য পাওয়া যায়, তবে অফিশিয়াল ডেটাবেজ হলো <https://lookup.icann.org/lookup>। তার বাইরে এই <http://onsameip.com.ipaddress.com> ওয়েবসাইট ব্যবহার করে অতিরিক্ত কিছু তথ্য পাওয়া যায়, যেমন একই আইপি অ্যাড্রেসের অধীনে কয়টি ওয়েবসাইট হোস্ট করা হয়েছে।

একটি টার্গেট ওয়েবসাইট বা প্রতিষ্ঠান সম্পর্কে Whois ব্যবহার করে কী কী তথ্য পাওয়া যায়, নিচে তার কিছু নমুনা তুলে ধরা হলো -

Nameserver:

dns2.xyzphosting.com 19X.1x8.x1.1x7

dns1.xyzphosting.com 19X.1x8.x1.1x8

DNSSEC Information:

Delegation Signed: Unsigned

Registrar Info:

Name Not a real company, PLC.

Whois Server whois.notarealcompany.com

Referral URL <http://notarealsolutions.com>

Registrant Contact Information

Name Mr X

Organization ABC Company

Address xxxx

City Dhaka

State / Province Dhaka

Postal Code 1215

Country BD

Phone +880.1234567890

Email unreal@abccompany.com

Administrative Contact Information:

Same as above

Technical Contact Information:

Same as above

Shodan

শোডান (<https://www.shodan.io/>) হলো ইন্টারনেটের সঙ্গে সরাসরি যেসব ডিভাইস যুক্ত আছে, সেগুলোকে নাম ধরে সন্ধান করার সাইট। গুগলে কোনো শব্দ লিখে সার্চ দিলে ওই শব্দ দিয়ে বানানো ওয়েবসাইট বা কনটেন্ট খুঁজে দেয়, তেমনি এখানে ওই শব্দ দিয়ে নাম রাখা যেকোনো ডিভাইস খুঁজে বের করে দেয়। এভাবে শোডান দিয়ে টার্গেট প্রতিষ্ঠানের কী কী ডিভাইসের সঙ্গে ইন্টারনেট থেকে সরাসরি যোগাযোগ স্থাপন করা যায় তা দেখা যায়। এগুলোর মধ্যে থাকতে পারে স্মার্ট টিভি, রাউটার, ইন্টারনাল সার্ভার, এমনকি প্রিন্টার বা সিসিটিভি ক্যামেরা – যা আমাদের আক্রমণের চমৎকার লক্ষ্যবস্তু হতে পারে। এসব ডিভাইস হ্যাক করে ওই প্রতিষ্ঠানের অভ্যন্তরীণ নেটওয়ার্কে অনুপ্রবেশ করা সম্ভব।

যেকোনো ডিভাইসের নাম লিখে অনুসন্ধানের ফলাফল কেমন হতে পারে তার নমুনা (আসল ফলাফল নয়) নিচে দেওয়া হলো :

```
x5.2x1.x8.2x1
client-45-2x1-x8-2x1.notsotech.net
Not so good technologies
Added on 20xx-03-22 03:03:58 GMT
Bangladesh
```

```
Firmware: 1
Hostname: this-is-my-device
Vendor: MicroTech
2x0.x.x3.2x0
2x0-x-x3-2x0-dsl.badinternet.com
Some Company Online Limited
Added on 20xx-04-07 15:03:33 GMT
Bangladesh, Dhaka
```

শোডানের মতো আরেকটি চমৎকার অনুসন্ধানী ওয়েবসাইট হলো <https://censys.io/>

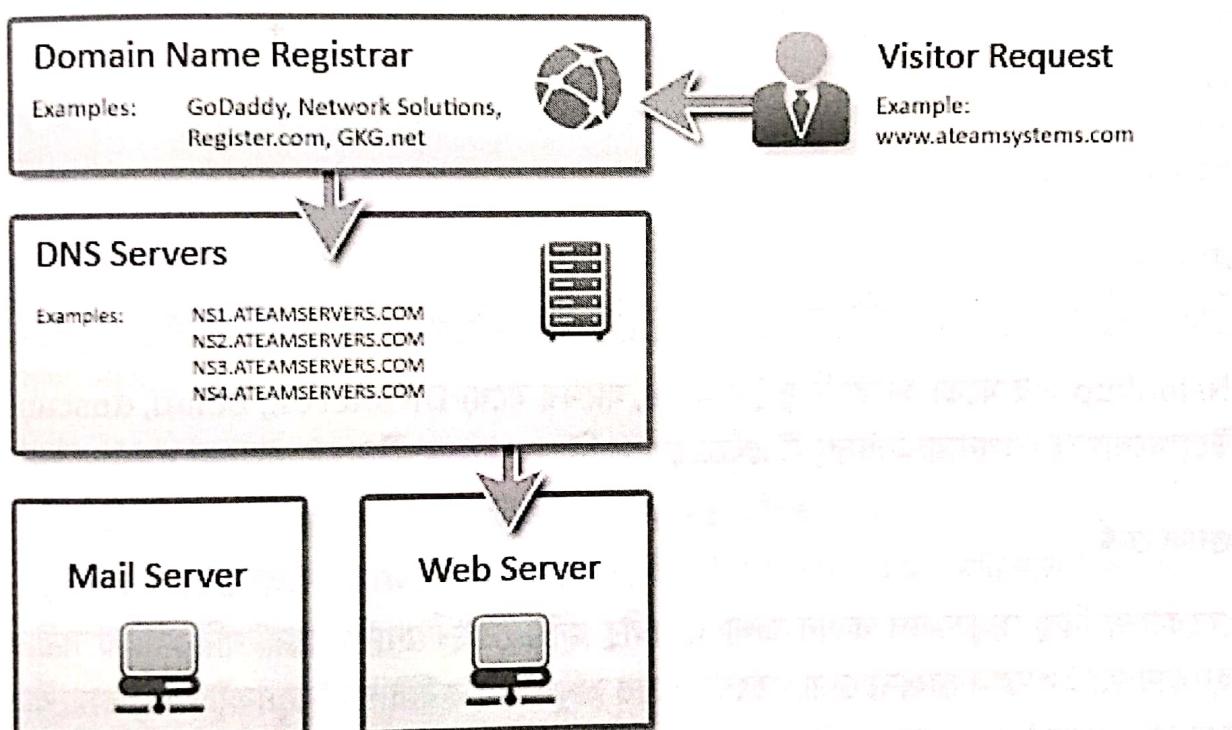
DNS

ডিএনএস সার্ভারে (সেটি নিজস্ব কিংবা অন্য কারো কাছ থেকে নেওয়া) ওই কোম্পানির সব অভ্যন্তরীণ সার্ভার বা নেটওয়ার্ক হোস্ট, যেমন- ইমেইল সার্ভার, ওয়েব সার্ভার, রাউটার, সুইচ ইত্যাদির আইপি অ্যাড্রেস-সম্পর্কিত তথ্য থাকে, যাদেরকে নেম রেকর্ড বলা হয়।

DNS সার্ভারে থাকা এসব তথ্য খুঁজে দেখার জন্য আমরা Nslookup টুল ব্যবহার করে থাকি।

Nslookup-এর বিভিন্ন কমান্ডের উদাহরণ হচ্ছে :

```
nslookup [-SubCommand ...] [{ComputerToFind| [-Server]}]
$ nslookup example.com (Find A record)
$ nslookup -type=ns example.com (Find NS record)
$ nslookup -type=soa example.com (Find SOA record)
$ nslookup -query=mx example.com (Find MX or email server record)
$ nslookup 10.20.30.40
$ nslookup -port=56 example.com
$ nslookup -debug example.com
```



ছবি 2.2

এসব কমান্ডের ফলাফল হতে পারে এরকম :

name	class	type	data	time to live
some-company.com (00:05:00)	IN	NS	a4-66.not-real.net	300s
some-company.com (00:05:00)	IN	NS	a10-66.not-real.net	300s
some-company.com (00:05:00)	IN	NS	a3-65.not-real.net	300s

some-company.com	IN	NS	a16-64.not-real.net	300s
(00:05:00)				
some-company.com	IN	NS	a11-67.not-real.net	300s
(00:05:00)				
some-company.com	IN	NS	a1-137.not-real.net	300s
(00:05:00)				
some-company.com	IN	A	1x4.50.2x8.27	20s
(00:00:20)				
some-company.com	IN	A	1x4.50.2x8.9	20s
(00:00:20)				
some-company.com	IN	SOA		
server:			a1-137.not-real.net	
email:			hostmaster@not-real.com	
serial:			2017011851	
refresh:			21600	
retry:			3600	
expire:			1209600	
minimum ttl:			300	
some-company.com	IN	MX		
preference:			10	
exchange:			mail.some-company.com	

Nslookup-এর মতো আরো কিছু টুল আছে, যাদের মধ্যে DNSRecon, Belati, dnsmap প্রভৃতি উল্লেখযোগ্য। আপনারা ইন্টারনেট থেকে জেনে নিতে পারেন কীভাবে এগুলো ব্যবহার করা হয়।

গুগল ডর্ক

যেকোনো কিছু অনুসন্ধান করার জন্য গুগলের জুড়ি নেই। হ্যাকিংয়ের পরিকল্পনা করার সময় হ্যাকাররাও গুগলের সাহায্য নেয়। তবে তাদের অনুসন্ধান করার পদ্ধতি একটু ভিন্ন, তারা যা খুঁজতে চায় তার সঙ্গে বিশের ফরম্যাটে আরো কয়েকটি শব্দ জুড়ে দেয়, যা গুগল ডর্ক (Google Dork) নামে পরিচিত। এই ডর্ক অপারেটর গুগলের সার্চ ইঞ্জিনকে কীভাবে বা কোন পরিধির ভেতরে অনুসন্ধান চালাবে তার নির্দেশনা দিতে পারে, যাতে অবাঞ্ছিত ফলাফল বাদ পড়ে যায়। এভাবে বিভিন্ন গুগল ডর্ক অপারেটর ব্যবহার করে টার্গেট ওয়েবসাইটের ভেতরে ফলপ্রসূ বিশেষায়িত অনুসন্ধান করা সম্ভব। যেমন :

- filetype:<extension> (যেমন .txt, .log, etc) নির্দিষ্ট কিছু ফাইল টাইপ খুঁজে বের করা
- intext: নির্দিষ্ট কিছু শব্দ আছে এমন কিছু খুঁজে বের করা

- intitle: প্রদত্ত শব্দগুলো আছে এমন টাইটেল যুক্ত পেজ খুঁজে বের করা
- inurl:<target URL> শুধু নির্দিষ্ট একটি ওয়েবসাইটের ভেতরে অনুসন্ধান সীমাবদ্ধ রাখা

আমরা <https://securitytrails.com/blog/google-hacking-techniques> এবং <https://www.exploit-db.com/google-hacking-database> এই দুটি ওয়েবসাইট ব্রাউজ করে এরকম আরো অনেক ডর্ক অপারেটরের ব্যবহার জানতে পারব। গুগলের মাধ্যমে এরকম বিশেষায়িত অনুসন্ধানে চালানোর সময় কখনো-বা এমন কিছু ফাইল বা পেজ হাতে চলে আসে, যাতে গোপনীয় বা মূল্যবান তথ্য, যেমন- লগ ফাইল, অভ্যন্তরীণ ইউজার আইডি, পাসওয়ার্ড, সার্টিফিকেট বা গোপন সংকেত, টেস্ট ডেটা, কাস্টমার তালিকা, ডিফল্ট সেটিংস, সিস্টেম কনফিগারেশন ইত্যাদি থাকতে পারে।

সোশ্যাল মিডিয়া

ফেসবুক, লিংকডইন, টুইটার, পিনটারেস্ট, টাম্বলার (Tumblr) ইত্যাদি সামাজিক যোগাযোগ মাধ্যমগুলোতে ব্যবহারকারীরা নিজের ব্যক্তিগত বা কর্মজীবনের অসংখ্য তথ্য শেয়ার করে থাকেন। তাদের প্রোফাইল আর পোস্ট ঘাঁটাঘাঁটি করে আমরা যেসব তথ্য পেতে পারি তার মধ্যে উল্লেখযোগ্য হচ্ছে :

- ফেসবুক - জন্মদিন, পারিবারিক সম্পর্ক, চেক-ইন স্থান, বর্তমান শহর ইত্যাদি।
- লিংকড-ইন - কর্মজীবন, প্রাতিষ্ঠানিক অবস্থান, সহকর্মী ইত্যাদি।
- টুইটার - ব্যক্তিগত বা রাজনৈতিক মতামত, বিতর্কিত বিষয়ে কেমন দৃষ্টিভঙ্গি ইত্যাদি।
- ইনস্টাগ্রাম/পিন্টারেস্ট - ব্যক্তিগত ছবি, ছুটিতে কোথায় বেড়াতে গেছেন ইত্যাদি।
- টাম্বলার বা অন্যান্য ব্লগ সাইট - দিনপঞ্জি, ভ্রমণ তালিকা, অন্যান্য অভিজ্ঞতা ইত্যাদি।

এসব মাধ্যম থেকে প্রাপ্ত তথ্যগুলো একসঙ্গে মিলিয়ে নিলে একজন ব্যক্তির পূর্ণাঙ্গ জীবনবৃত্তান্ত অথবা গত কয়েক বছরের কর্মকাণ্ডের রূপরেখা দাঁড় করানো যায়, যা ব্যবহার করে তার অ্যাকাউন্টের গোপন প্রশ্ন, ফাঁস হওয়া পাসওয়ার্ড ইত্যাদি অনুমান করার চেষ্টা করা যায়। ব্যক্তিগত তথ্য হাতের কাছে থাকলে তার পরিচিত কাউকে তার মানে প্রতারণামূলক ইমেইল করে, বার্তা পাঠিয়ে বা কল দিয়ে বোকা বানানো সম্ভব; এরকম বোকা বানানোর প্রচেষ্টাকে বলা হয় সোশ্যাল ইঞ্জিনিয়ারিং। হ্যাকাররা ওই ব্যক্তিকে তার প্রতিষ্ঠানের আইটি সাপোর্ট বা ব্যাংকের কল সেন্টার এজেন্ট সেজে ভুয়া ফোন কল করে নিজেকে বিশ্বাসযোগ্যভাবে উপস্থাপন করে, জরুরি কোনো সমস্যা হয়েছে জানিয়ে তার অ্যাকাউন্টের তথ্য হাতিয়ে নিতে পারে। একইভাবে তার পরিচিত কারো কাছে কাছাকাছি নামে ইমেইল করে বা সোশ্যাল মিডিয়াতে মেসেজ পাঠিয়ে কাউকে বিশেষ

কোনো লিংকে ক্লিক করতে প্রলুক্ষ করে তার মাধ্যমে সিস্টেম অ্যাক্সেস গ্রহণ, পাসওয়ার্ড চুরি করা বা ক্ষতিকারক সফটওয়্যার ইনস্টল করানো খুব বেশি কঠিন হবে না।

বিভিন্ন সামাজিক যোগাযোগ মাধ্যমে এভাবে কষ্ট করে এত প্রোফাইল খুঁজতে না চাইলে বিকল্প হিসেবে Jigsaw (<https://www.jigsawsecurityenterprise.com/>) ব্যবহার করে বেশ সহজে একটি প্রতিষ্ঠানের কর্মীদের সম্পর্কে তথ্য সংগ্রহ করা সম্ভব। একই সঙ্গে কালি লিনাক্স থেকে সোশ্যাল ইঞ্জিনিয়ারিং টুলকিট (<https://github.com/trustedsec/social-engineer-toolkit>) ব্যবহার করে যেকোনো প্রতিষ্ঠানের কর্মীরা নকল ইমেইল আক্রমণ সম্পর্কে কেমন সচেতন, তা যাচাই করার জন্য অবিকল নকল সাইট বানিয়ে নানা রকম সিমুলেশন টেস্ট করা যায়।

ওয়েবসাইট প্লাটফরম

নেটক্রাফট (<https://sitereport.netcraft.com/>) ব্যবহার করে টার্গেট ওয়েবসাইট প্লাটফরম সম্পর্কে অনেক তথ্য পাওয়া যায়, যেমন :

- Background - সাইটের পরিচিতি
- Network - নেম সার্ভার, আইপি অ্যাড্রেস ইত্যাদি হোস্টিং-সম্পর্কিত তথ্য
- Hosting History - হোস্ট করার পর আইপি অ্যাড্রেস কখন কার কাছ থেকে নেওয়া
- SSL/TLS - কেমন এনক্রিপশন প্রটোকল ব্যবহৃত হয়েছে বা দুর্বলতা আছে কি না
- Sender Policy Framework, DMARC - ইমেইল নিরাপত্তা
- Web Trackers - কী কী তৃতীয় পক্ষের ট্র্যাকিং লাইব্রেরি আছে
- Site Technology - কেমন ধরনের ওয়েব টেকনোলজি ব্যবহৃত হয়েছে

নেটক্রাফটের ডিএনএস সার্চ (<https://searchdns.netcraft.com/>) অপশন ব্যবহার করে একই আইপি অ্যাড্রেসে আর কী কী ওয়েবসাইট হোস্ট করা হয়েছে তা জানা যায়।

BuiltWith (<https://builtwith.com/>) দিয়ে একটি ওয়েবসাইটে কী কী টেকনোলজি বা প্লাগইন ব্যবহার করা হয়েছে তার হিসেবের করা যায়, যা অনেকটা ছবি 2.3-এর মতো দেখা যাবে।

হ্যাকাররা তারপর এসব প্লাগইন সম্পর্কে আরো তথ্য জোগাড় করে তাদের কোনো দুর্বলতা আছে কি না তা যাচাই করে বুঝতে পারে।

ওয়েবসাইটের ইতিহাস

যেকোনো কোম্পানির ওয়েবসাইট প্রতিনিয়ত পরিবর্তিত হয়, তাতে নতুন নতুন তথ্য যুক্ত করা হয়, আবার পুরোনো তথ্য মুছে ফেলা হয়। আজ থেকে বছর দুয়েক আগে সেই ওয়েবসাইটটি ঠিক কেমন ছিল সেটি জানার জন্য Wayback machine (<https://archive.org/>) খুবই উপকারী একটি সাইট। সময়ে সময়ে তারা সারা দুনিয়ার কোটি কোটি ওয়েবসাইটের স্ন্যাপশট নিয়ে সেগুলো তাদের আর্কাইভে সংরক্ষণ করে রাখে। এসব স্ন্যাপশট দেখে কোনো অতীতের কোনো এক সময় একটি ওয়েবসাইটে কী তথ্য ছিল বা কী কী পরিবর্তন হলো সেগুলো খুঁজে দেখা সম্ভব।

Analytics and Tracking	First Detected	Last Detected	
Chartbeat Visitor Count Tracking	Jan 2011	Jan 2019	⌚ \$
Google Analytics Application Performance - Audience Measurement - Visitor Count Tracking	Jan 2011	Jan 2019	⌚
Google Analytics Classic	Sep 2015	Jan 2019	⌚
Global Site Tag	Dec 2017	Jan 2019	⌚
Facebook Domain Insights Social Management	Jul 2013	Jul 2018	⌚
comScore Advertiser Tracking - Audience Measurement - Conversion Optimization - Site Optimization - Visitor Count Tracking	Aug 2014	Jul 2018	⌚
Alexa Certified Site Metrics Audience Measurement - Visitor Count Tracking	Aug 2013	Apr 2018	⌚ \$
Google Universal Analytics	Sep 2014	Apr 2018	⌚
New Relic Application Performance	Jan 2015	Mar 2018	⌚
Alexa Metrics Visitor Count Tracking	Aug 2013	Dec 2017	⌚
Google Analytics with Ad Tracking Advertiser Tracking	Jan 2014	Dec 2017	⌚
Everest Technologies	Nov 2014	Sep 2017	⌚ \$
DoubleClick Floodlight	Dec 2014	May 2017	⌚
Lotame Crowd Control	May 2014	Feb 2017	⌚
MediaMath Advertiser Tracking - Demand-side Platform	Jul 2014	Feb 2017	⌚
Netmining Marketing Automation	Nov 2014	Feb 2017	⌚ \$
Rapleaf Marketing Automation	Jan 2016	Feb 2017	⌚ \$

ছবি 2.3

Enumeration

Enumeration হলো সন্তাব্য ইউজার অ্যাকাউন্ট সম্পর্কে তথ্য জোগাড় করা। এক্ষেত্রে নিচের কয়েকটি উপায় অবলম্বন করা যেতে পারে :

- HaveIBeenPwned (<https://haveibeenpwned.com/>) হলো ফাঁস ইওয়া ইমেইল বা অন্যান্য খবরের এক বিশাল ভান্ডার। যদি আমাদের টার্গেট কোম্পানির কোনো কর্মী ফাঁস হয়ে যাওয়া পাসওয়ার্ড বদলে না থাকেন, তবে তো হয়েই গেল, আর বদলে না ফেললেও ইউজার আইডি বা পাসওয়ার্ড প্যাটার্ন দেখে তার নতুন পাসওয়ার্ড কেমন তা অনুমান করার চেষ্টা তো করা যেতে পারে।
- কোনো একটি বিশেষ ইউজার নেম ব্যবহার কোন কোন সোশ্যাল মিডিয়াতে অ্যাকাউন্ট খোলা হয়েছে সেটা খুঁজে দেখে বা একই ইমেইল দিয়ে কতগুলো অ্যাকাউন্ট খোলা হয়েছে তা যাচাই করার জন্য ওপরের সাইটটি ব্যবহার করা যায়।
- কোনো প্রতিষ্ঠানের বিভিন্ন ক্লাউড সার্ভিস অ্যাকাউন্ট, যেমন AWS S3, Git repository ইত্যাদির পাবলিক সেকশন খুঁজে দেখতে হয় যে ভুলক্রমে কেউ গোপন সংকেত, পাসওয়ার্ড, শেয়ারড অ্যাকাউন্ট শেয়ার দিয়ে রেখেছে কি না।
- সেই সঙ্গে বিভিন্ন সার্ভার অ্যাপ্লিকেশনের ডিফল্ট ইউজার নেম ও পাসওয়ার্ডের তালিকা সংগ্রহ করাও জরুরি, কারণ অনেকেই এখনো সেগুলোই ব্যবহার করে যাচ্ছেন!

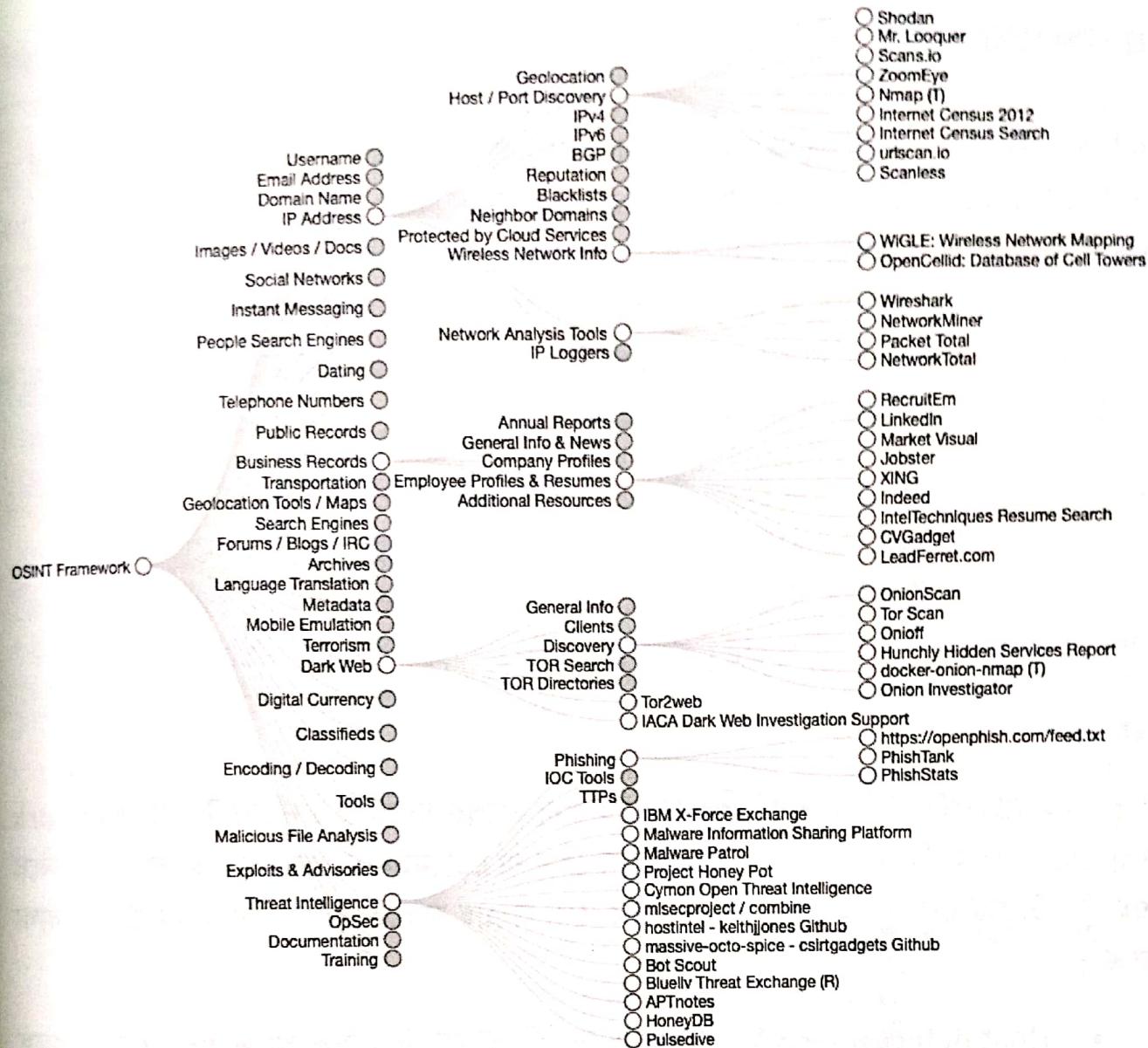
OSINT ফ্রেমওয়ার্ক

সরাসরি কোনো টুল না হলেও এই ওয়েবসাইটে (<http://osintframework.com/>) কীভাবে কোন উৎস থেকে কী ধরনের তথ্য সংগ্রহ করা যায়, তা বিষয়ভিত্তিক বিভিন্ন ক্যাটাগরিতে ভাগ করে খুব সুন্দরভাবে ছবির মতো করে সাজানো আছে (ছবি 2.4)। এই সাইটে গিয়ে বিভিন্ন উৎস-পয়েন্টে ক্লিক করে সেটি কোথায় আছে, তার ঠিকানা জানা যায়, আর দরকারমতো সেই টুল সঙ্গে সঙ্গে ওপেন করে নিয়ে বিভিন্ন তথ্য খুঁজে নেওয়া যায়।

যাচাই করে নিন (Test your knowledge)

ধরুন একজন হ্যাকারের টার্গেট হলো কোনো প্রতিষ্ঠানের অর্থ বিভাগের গুরুত্বপূর্ণ একজন কর্মীর আইডি পাসওয়ার্ড হাতিয়ে নেওয়া। তাহলে শুধু পরোক্ষভাবে তথ্য জোগাড় করে কীভাবে সেটা করা সন্তুষ্ট? এই কাজের জন্য তার তথ্যসূত্র জোগাড় এবং সন্তাব্য পরিকল্পনার প্রতিটি ধাপ চিন্তা করে বের করে লিখে ফেলুন তো!

অধ্যায় ২ – হ্যাকিংয়ের পরিকল্পনা



ছবি 2.4

সারসংক্ষেপ

দেখলেন তো, টার্গেট সিস্টেমে একদম হাত না দিয়ে কত বিচ্ছিন্ন তথ্যই না সংগ্রহ করা যায়! এই তথ্য বিশ্লেষণ করে আমরা টার্গেট সিস্টেমের গঠন, কী প্রযুক্তি ব্যবহৃত হয়েছে, ইউজার কারা, কী কী ডিভাইস ইন্টারনেট থেকে সরাসরি দেখা যায়, আইপি অ্যাড্রেস রেঞ্জ, হোস্টিং সার্ভার, কোনো অভ্যন্তরীণ ডিরেক্টরি বা ফাইল ভুলবশত পাবলিক করা আছে কি না, এ রকম অনেক কিছু জেনে নিতে পারব। এমনকি কপাল ভালো হলে ইউজার আইডি, পাসওয়ার্ড কিংবা অ্যাপ্লিকেশনের গোপন সংকেত পর্যন্ত হাতে চলে আসতে পারে। কাজেই বুঝতেই পারছেন, আসল হ্যাকারুরাও কিন্তু এভাবেই মূল সিস্টেমে না ঢুকেই অনেক তথ্য হাতিয়ে নেয়, যা ব্যবহার করে তাদের জন্য আক্রমণ পরিকল্পনা করা অনেকটাই সহজ হয়ে যায়।

প্রত্যক্ষ তথ্য সংগ্রহ

প্রত্যক্ষভাবে তথ্য সংগ্রহের (Active reconnaissance) জন্য টার্গেট কোম্পানির নেটওয়ার্ক বা অন্যান্য সিস্টেমের সঙ্গে কিছু বিশেষ বার্তা আদান-প্রদান করে, ওয়েবসাইটের প্রতিটি পেজ অফ তাম করে খুঁজে দেখে অথবা নেটওয়ার্ক স্ক্যান করে বের করা হয় কী কী সার্ভিস চালু আছে, সেখানে ব্যবহৃত অপারেটিং সিস্টেম ও অ্যাপ্লিকেশনের ভার্শন কত, কী ধরনের প্লাটফরম বা ফ্রেমওয়ার্ক ব্যবহৃত হচ্ছে ইত্যাদি। এসব তথ্য একসঙ্গে মিলিয়ে ওয়েব অ্যাপ্লিকেশন বা নেটওয়ার্ক আর্কিটেকচার সম্পর্কে বেশ পরিষ্কার ধারণা পাওয়া যায়।

প্রত্যক্ষ তথ্য সংগ্রহ করার জন্য যেসব টুল লাগবে সেগুলো একসঙ্গে কালি লিনাক্সে আগে থেকেই ইনস্টল করে ক্যাটাগরি অনুযায়ী সাজিয়ে মেনুতে চমৎকারভাবে সন্নিবিষ্ট করে দেওয়া আছে। লিনাক্সের এই ডিস্ট্রিবিউশনটি কীভাবে ইনস্টল এবং সেটআপ করতে হবে, সেটি আমরা পরবর্তী অধ্যায়ে শিখে নেব। তার আগে এই টুলগুলোর সংক্ষিপ্ত পরিচয় জেনে নেওয়া যাক।

NMap

Nmap হলো নেটওয়ার্ক সার্ভিস নিরীক্ষা করার জন্য বিশ্বের সবচেয়ে জনপ্রিয় টুল, যা 'Network Mapper'-এর সংক্ষিপ্ত নাম। আইপি অ্যাড্রেস রেঞ্জ বা ডোমেইনকে লক্ষ্যবস্তু হিসেবে ধরে নিয়ে এই টুল টার্গেট নেটওয়ার্ক স্ক্যান করে যেসব তথ্য সংগ্রহ করতে পারে তার মধ্যে উল্লেখযোগ্য হচ্ছে :

- Host detection - একটি নেটওয়ার্কের কী কী হোস্ট লাইভ আছে এবং তাদের কাছে ICMP বা TCP প্যাকেট পাঠিয়ে তাদের সাড়া কেমন তা পরীক্ষা করতে পারে।
- IP and DNS information detection - কোন নেটওয়ার্কে যুক্ত থাকা বিভিন্ন ধরনের ডিভাইসের ম্যাক অ্যাড্রেস, আইপি অ্যাড্রেস বা রিভার্স ডিএনএস ইত্যাদি তথ্য সংগ্রহ করতে পারে।
- Port detection - ওই নেটওয়ার্কে কোন কোন পোর্ট চালু আছে, এবং সেখানে সম্ভাব্য কী কী সার্ভিস চলছে সে সম্পর্কে ধারণা দিতে পারে।
- OS detection - হোস্টগুলোতে কোন অপারেটিং সিস্টেম চলছে, তাদের ভার্শন কী এবং হার্ডওয়ার টাইপ সম্পর্কে ধারণা দিতে পারে।
- Version detection - বিভিন্ন সার্ভিসের পেছনে যে অ্যাপ্লিকেশন চলছে তাদের ভার্শন সম্পর্কেও বেশ নির্ভরযোগ্য তথ্য দিতে পারে।

পিং (Ping)

পিং কমান্ড তেমন গোপনীয় কোনো তথ্য না দিলেও টার্গেট নেটওয়ার্কের বিভিন্ন হোস্ট কেমন সাড়া দেয় এবং হোস্ট পর্যন্ত পৌছাতে কয়টি হপ (hop) পার হতে হয়, তা যাচাই করতে ব্যবহার করা যেতে পারে। উইন্ডোজ থেকে পিং করলে নিচের মতো আউটপুট আসবে :

```
Pinging not-a-realcompany.com [7x.2x6.64.2x4] with 32 bytes of data...
```

```
Reply from 7x.2x6.64.2x4: bytes=32 time=215ms TTL=49
```

```
Reply from 7x.2x6.64.2x4: bytes=32 time=216ms TTL=49
```

```
Reply from 7x.2x6.64.2x4: bytes=32 time=213ms TTL=49
```

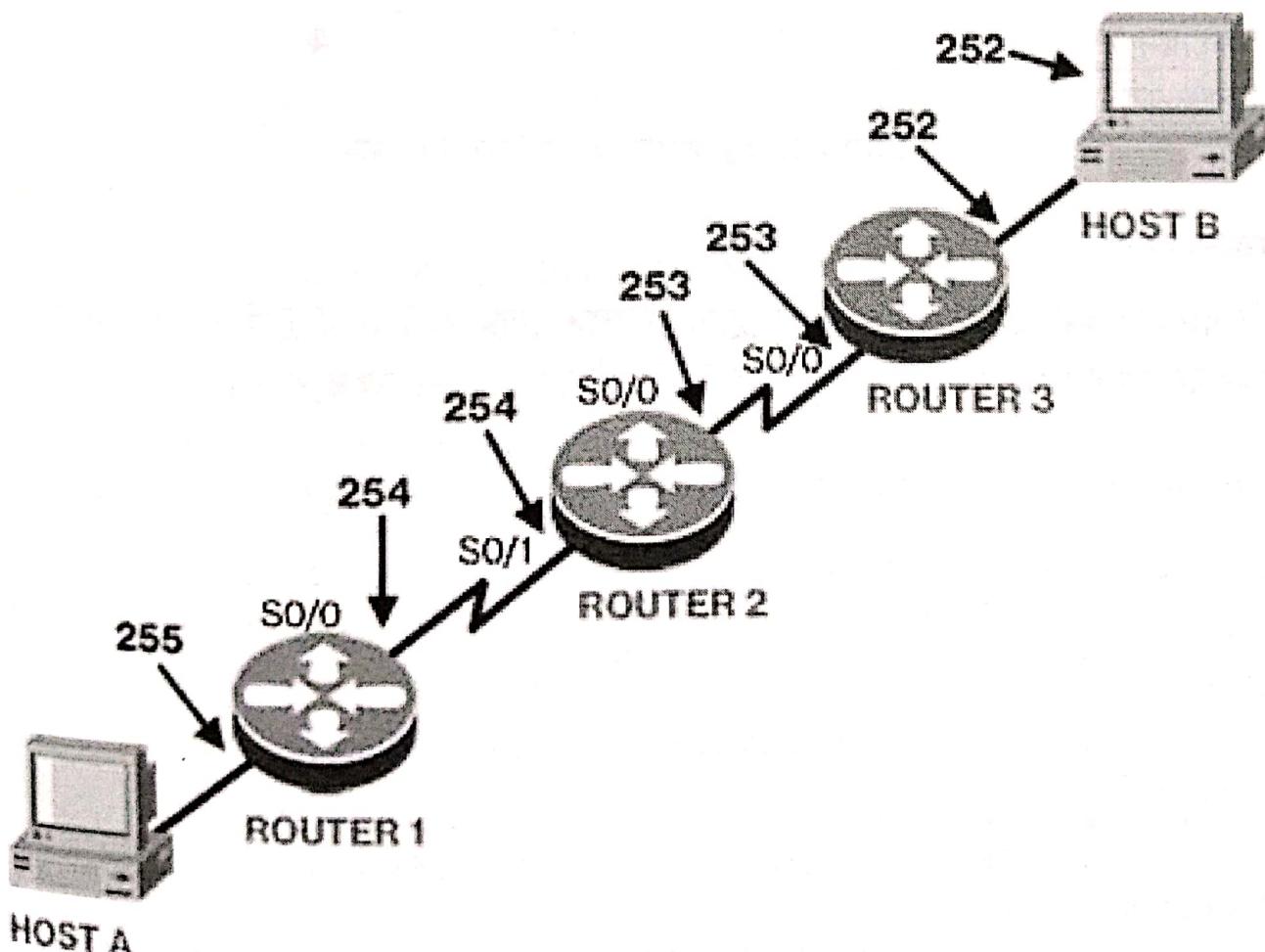
```
Reply from 7x.2x6.64.2x4: bytes=32 time=214ms TTL=49
```

```
Ping statistics for 7x.2x6.64.2x4:
```

```
    Packets: Sent = 4, Received = 4, Lost = 8 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 213ms, Maximum = 216ms, Average = 214ms
```



ছবি 2.5: প্রত্যেক রাউটারের প্রত্যেক ইন্টারফেসের TTL মান

এই TTL (Time to live-এর মানে হলো ডেস্টিনেশনে পৌঁছাতে সর্বোচ্চ কতগুলো হপ পার হয়ে যেতে পারবে, এই সীমা পার হয়ে গেলে রাউটার সেই নেটওয়ার্ক বার্তা বাতিল করে দেয়) ভ্যালু একেক অপারেটিং সিস্টেমে একেক রকম হয় বলে এটি দেখেও কিন্তু কোন ধরনের অপারেটিং সিস্টেম চলছে সে সম্পর্কে ধারণা পাওয়া যেতে পারে। তবে OS ভার্শন বদলে গেলে ভ্যালু বদলে যায়, তাই নিচের টেবিল থেকে প্রাথমিক ধারণা নেওয়া যেতে পারে কিন্তু নিশ্চিত হতে অন্যান্য টুলের আউটপুট দেখতে হবে।

অপারেটিং সিস্টেম	TTL
লিনাক্স (Linux) (কোর্নেল 4.10)	64
ফ্রিবিএসডি (FreeBSD)	64
অপেনবিএসডি (OpenBSD)	64
উইন্ডোজ 2000	128
উইন্ডোজ এক্সপি, ভিস্টা, 7, 10	128
উইন্ডোজ সার্ভার 2008	128
সিসকো রাউটার আইওএস 12.4	255
সোলারিস 7	255
ম্যাকওএস	64

টেবিল 2.1: কিছু অপারেটিং সিস্টেমের TTL মান

Traceroute

এটি ব্যবহার করে হোস্ট থেকে লক্ষ্যবস্তুতে পৌঁছুতে গেলে নেটওয়ার্ক ট্রাফিক কোন রুটে যায়, মাঝখানে কোন কোন প্রোভাইডার বা হোস্ট আছে ইত্যাদি দেখা যেতে পারে।

Tracing route to some-company.com [7x.2x6.6x.2x6]...						
Hop	rtt	rtt	rtt	ip address	fully qualified domain name	
1	1	1	1	1x9.254.1x8.58		
2	1	1	1	1x9.48.1x8.1x8	ae103.ppr02.dal13.some-	
layer.com						
3	0	0	0	1x9.48.1x8.1x8	8a.76.30a9.ip4.static.some-	
reverse.com						
4	*	*	*			
5	7	7	8	1x9.45.1x.142	ae3.cbs02.sr02.hou02.some-	
layer.com						
6	8	9	7	1x9.45.1x.120	ae7.cbs01.sr02.hou02.some-	
layer.com						

অধ্যায় ২ – হ্যাকিংয়ের পরিকল্পনা

```
1      30    31    30    1x9.45.1x.1x5    ae0.cbs01.tm01.mia01.some-
layer.com
2      30    30    30    1x9.45.1x.1x9    81.12.2da9.ip4.static.some-
reverse.com
3      32    31    30    2x6.41.1x8.17    coresite-
mia2.netarch.somenetwork.com
4      30    30    30    72.246.64.226
a7x-2x6-xx-2x6.deploy.static.somenetworktechnologies.com
```

Netcat

টার্গেট নেটওয়ার্কে বিভিন্ন কমান্ড পাঠানো এবং সেখান থেকে কেমন সাড়া পাওয়া যায় তা দেখার জন্য নেটক্যাট (<https://nmap.org/ncat/>) বেশ ভালো একটি সফটওয়্যার।

Wireshark

ওয়ারশার্কের (<https://www.wireshark.org/>) কথা না বললেই নয়। যেকোনো নেটওয়ার্কের ভেতরে বিভিন্ন প্রটোকলের মাধ্যমে যেসব প্যাকেট বা বার্তা আদান-প্রদান হয়, সেগুলোর খুঁটিনাটি বিশ্লেষণ করার জন্য এটি এক অসাধারণ সফটওয়্যার।

OpenVAS

ওয়েব অ্যাপ্লিকেশন স্ক্যান করার জন্য খুব জনপ্রিয় ফ্রি টুল হচ্ছে OpenVAS (<https://www.openvas.org/>), যা টার্গেট ওয়েবসাইট ঘেঁটে স্বয়ংক্রিয়ভাবে বিভিন্ন দুর্বলতা খুঁজে বের করতে পারে। এর বিস্তারিত ব্যবহার আমরা পরে শিখব।

SQLmap

ওয়েব অ্যাপ্লিকেশন যেসব তথ্য প্রদর্শন করে থাকে তা খুঁজে আনার জন্য সার্ভার ডেটাবেজের সঙ্গে যোগাযোগ করে। হ্যাকাররা ওয়েবসাইটের POST/GET মেসেজের মাঝে কিছু বিশেষ এসকিউএল কমান্ড পাঠিয়ে দেয় যা অনেক সময় ডেটাবেজ সার্ভারকে বিভ্রান্ত করে দিয়ে সাধারণ তথ্যের বাইরে অন্যান্য তথ্য দিতে বাধ্য করে। এভাবে বার্তার ভেতর এসকিউএল কমান্ড পাঠানোর ঘটনাকে বলা হয় এসকিউএল ইনজেকশন (SQL injection)। কোনো ওয়েব অ্যাপ্লিকেশন এসকিউএল ইনজেকশনের শিকার হবে কি না সেটি যাচাই করতে sqlmap টুল বেশ পারঙ্গম।

Enumeration

সিস্টেমে সংরক্ষিত অ্যাকাউন্ট-সম্পর্কিত তথ্য, যেমন- আইডি, পাসওয়ার্ড, হ্যাশ ভ্যালু, প্রিভিলেজ লেভেল, এনক্রিপশন সংকেত ইত্যাদি খুঁজে বের করা অথবা সেগুলো ব্যবহার করে বৈধ ইউজার হিসেবে নেটওয়ার্ক সার্ভিস অ্যাঞ্জেলের চেষ্টা করার জন্য DNS Recon, AutoRecon, Nmap, AutoScan, wpscan, Nikto, Dirbuster ইত্যাদি টুল ব্যবহার করা হয়।

যাচাই করে নিন (Test your knowledge)

ইন্টারনেট ঘেঁটে উপর্যুক্ত টুলগুলোর উইন্ডোজ ভার্শন আছে কি না দেখে নিতে পারেন। চাইলে দু-একটি টুল (যেমন, zenmap) চালিয়েও দেখতে পারেন।

সারসংক্ষেপ

পরোক্ষভাবে প্রাপ্ত তথ্য (বিশেষ করে ব্ল্যাক বস্র টেস্টিংয়ের ক্ষেত্রে যখন আর কিছুই জানা নেই) ব্যবহার করে টার্গেট সিস্টেমের ওয়েব প্লাটফরম এবং আইপি রেঞ্জ সম্পর্কে ধারণা পাওয়া যায়। তারপর কিছু পোর্ট স্ক্যানিং করে কী কী সার্ভিস চলছে, তাদের ভার্শন কত ইত্যাদি জানা যায়। এভাবে প্রত্যক্ষ ও পরোক্ষ দুভাবেই প্রাপ্ত তথ্যসূত্র থেকে প্রতিষ্ঠানের ওয়েব সার্ভিস ব্যবহারকারী বা সার্ভিসগ্রহীতা কারা, তারা কীভাবে অ্যাপ্লিকেশন অ্যাকসেস করে, প্রতিষ্ঠানের ওয়েবসাইটে ঘেঁটে সেখানে কী কী উন্মুক্ত ফাইল বা অন্যান্য দরকারি তথ্য দেওয়া আছে, ওয়েবসাইটে কী কী প্লাগইন বা তৃতীয় পক্ষের লাইব্রেরি ইনস্টল করা আছে, ব্রাউজার বা ক্লায়েন্ট সাইডে কী কী স্ক্রিপ্ট চলে এবং অনেক কিছু সম্পর্কে বিস্তারিত জানা যায়।

এসব তথ্য ব্যবহার করে ওই প্রতিষ্ঠানের ওয়েব এবং নেটওয়ার্ক সিস্টেমে কী কী দুর্বলতা থাকা সন্দেহ, সেখানে অনুপ্রবেশের উপায় কী হতে পারে বা ঠিক কী ধরনের আক্রমণ করা উচিত (যেমন, লিনাক্স বা উইন্ডোজের জন্য একই পদ্ধা কাজ করবে না) তা বিশ্লেষণ করে আক্রমণের পরিকল্পনা করা যায়।