**NMAP Zombie Scan**

**Nmap**: Nmap হচ্ছে একটি নেটওয়ার্ক ইউটিলিটি টুলস যেটার ফুল ফর্ম হচ্ছে নেটওয়ার্ক ম্যাপার এটি নেটওয়ার্ক স্ক্যানিং করে থাকে । যার মাধ্যমে আমরা যেকোনো ওয়েবসাইট অথবা আইপি এড্রেস স্ক্যান করতে পারি। এর মাধ্যমে আমরা কোনো ওয়েবসাইট এর কয়টি পোর্ট আছে এবং কোন পোর্ট খোলা আছে আর কোন পোর্ট বন্ধ আছে সেটা চেক করতে পারি। Zombie scan হলো nmap এর একটি স্ক্যান। নিম্নে এই বিষয়ে সংক্ষিপ্ত আলোচনা করা হলো।

**Zombie Scan:** Zombie scan হলো nmap একটি স্ক্যান, যার মাধ্যমে আমরা নিজের ডিভাইস এর আইপি ব্যাতিত অন্য ডিভাইস এর আইপি ব্যাবহার করে টার্গেট ডিভাইস কে স্ক্যান করতে পারি। এবং টার্গেট ডিভাইসকে রিকুয়েস্ট পাঠাতে পারি। Zombie scan ব্যবহার করলে টার্গেট ডিভাইস কখনো আমার আসল ডিভাইস কে ডিটেক্ট করতে পারবে না। আবার কোনো কোনো ক্ষেত্রে যদি টার্গেট আইপি ফায়ার ওয়াল দ্বারা সুরক্ষিত থাকে তাহলে আমরা সেখানে nmap স্ক্যান করতে পারি না। সেক্ষেত্রে আমরা যদি ওই আইপি এর সাথে সংশ্লিষ্ট অন্য কোনো আইপি পাই যেটা ফায়ার ওয়াল দ্বারা সুরক্ষিত নয় তাহলে সেই আইপি কে Zombie হিসেবে ব্যবহার করে সুরক্ষিত আইপি কে টার্গেট করতে পারি। তাহলে ফায়ার ওয়াল কখনো সেটা বুঝতে পারবে না।আইডি নিষ্ক্রিয় স্ক্যান কার্যকর করার প্রথম ধাপ হল একটি উপযুক্ত জম্বি খুঁজে পাওয়া।এটিকে বিশ্বব্যাপী (প্রতি হোস্টের সাথে যোগাযোগের পরিবর্তে) ভিত্তিতে আইপি আইডি প্যাকেটগুলি ক্রমবর্ধমানভাবে বরাদ্দ করতে হবে।যখন একটি নিষ্ক্রিয় স্ক্যান করার চেষ্টা করা হয়, Nmap প্রস্তাবিত জম্বি পরীক্ষা করে এবং এটির সাথে কোনো সমস্যা রিপোর্ট করে। যদি একটি কাজ না করে, অন্য চেষ্টা করুন।আপনার উৎস ঠিকানার কাছাকাছি বা লক্ষ্যের কাছাকাছি একটি নেটওয়ার্ক বেছে নেওয়া ভালো ফলাফল দেয়। আপনি পিং স্ক্যান ফলাফল থেকে প্রতিটি উপলব্ধ হোস্ট ব্যবহার করে একটি নিষ্ক্রিয় স্ক্যান করার চেষ্টা করতে পারেন যতক্ষণ না আপনি কাজ করে এমন একটি খুঁজে পান।

**Idle Zombie Scan Nmap এর সুবিধাঃ** আইডিলস্ক্যানের আইপি অ্যাড্রেস স্পুফ করার পদ্ধতি nmap-কে দূর থেকে খোলা পোর্ট খুঁজে বের করার অনুমতি দেয়, এমনকি যদি প্যাকেট ফিল্টার থাকে। যোগাযোগ প্রক্রিয়া সম্পূর্ণ করার জন্য Nmap-এর সহজভাবে একটি জম্বি ওয়ার্কস্টেশনে যেকোন খোলা পোর্ট প্রয়োজন। আইডলস্ক্যানের সবচেয়ে বড় সুবিধা হল স্টিলথ ফ্যাক্টর। একটি গন্তব্য স্টেশন কখনই nmap স্টেশনের IP ঠিকানা দেখতে পাবে না।

**Idle Zombie Scan Nmap এর অসুবিধাঃ** Idlescan শুধুমাত্র পোর্ট সনাক্ত করে। Idlescan কোনো অ্যাপ্লিকেশন সংস্করণ তথ্য বা অপারেটিং সিস্টেম ফিঙ্গারপ্রিন্টিং প্রদান করতে পারে না।

জম্বি অবশ্যই একটি নিষ্ক্রিয় স্টেশন হতে হবে এবং এটি নিশ্চিতভাবে জানা কঠিন। প্রায়শই, একটি উপযুক্ত নিষ্ক্রিয় স্টেশন চিহ্নিত করার আগে অনেকগুলি বিভিন্ন ডিভাইস idlescan দিয়ে পরীক্ষা করা হবে

স্পুফড আইপি ফ্রেম তৈরি করতে Idlescan-এর বিশেষাধিকারপ্রাপ্ত অ্যাক্সেস প্রয়োজন। বিশেষাধিকারপ্রাপ্ত অ্যাক্সেস ছাড়া, এই স্ক্যান চালানো হবে না।