THESIS PAPER

Submitted From:
FAHAD AHMED

CANADIAN UNIVERSITY OF BANGLADESH

নিষ্ক্রিয় স্ক্যান(Idle Scan)-

নিষ্ক্রিয় স্ক্যান একটি টিসিপি পোর্ট স্ক্যান পদ্ধতি যা কোন পরিষেবা পাওয়া যায় তা খুঁজে বের করার জন্য একটি কম্পিউটারে নকল প্যাকেট পাঠানো নিয়ে গঠিত। এটি অন্য কম্পিউটারের ছদ্মবেশ ধারণ করে সম্পন্ন হয় যার নেটওয়ার্ক ট্র্যাফিক খুব ধীর বা অস্তিত্বহীন (অর্থাৎ তথ্য প্রেরণ বা গ্রহণ না করা)। এটি একটি নিষ্ক্রিয় কম্পিউটার হতে পারে, যাকে "**জম্বি**" বলা হয়।

এই কাজটি সাধারণ সফ্টওয়্যার নেটওয়ার্ক ইউটিলিটি যেমন nmap এবং hping এর মাধ্যমে করা যেতে পারে। আরেকটি জম্বি মেশিনের স্বতন্ত্র বৈশিষ্ট্য খুঁজে বের করার প্রচেষ্টায় একটি নির্দিষ্ট মেশিনের লক্ষ্যবস্তুতে জাল প্যাকেট পাঠানো জড়িত। আক্রমণটি অত্যাধুনিক কারণ আক্রমণকারী কম্পিউটার এবং টার্গেটের মধ্যে কোন মিথস্ক্রিয়া নেই: আক্রমণকারী শুধুমাত্র "জম্বি" কম্পিউটারের সাথে যোগাযোগ করে।

এটি পোর্ট স্ক্যানার এবং মেশিনের মধ্যে বিশ্বস্ত আইপি সম্পর্কের ম্যাপার হিসাবে দুটি উদ্দেশ্যে কাজ করে। টার্গেট সিস্টেম "জম্বি" কম্পিউটারের সাথে ইন্টারঅ্যাক্ট করে এবং বিভিন্ন কম্পিউটারে টার্গেট দ্বারা প্রদত্ত বিভিন্ন বিশেষাধিকার প্রমাণ সহ বিভিন্ন "জম্বি" ব্যবহার করে আচরণের পার্থক্য লক্ষ্য করা যায়।

নিষ্ক্রিয় স্ক্যানের পিছনে সামগ্রিক উদ্দেশ্য হল "লক্ষ্যবস্তু হোস্টের কাছে সম্পূর্ণ অদৃশ্য থাকা অবস্থায় বন্দরের অবস্থা পরীক্ষা করা।"

একটি জম্বি হোস্ট খোঁজা(Finding a zombie host)-

একটি নিষ্ক্রিয় স্ক্যান চালানোর প্রথম পদক্ষেপ হল একটি উপযুক্ত জম্বি খুঁজে বের করা। আইপি আইডি প্যাকেটগুলিকে ক্রমবর্ধমানভাবে একটি বিশ্বব্যাপী (প্রতি হোস্টের পরিবর্তে এটি যোগাযোগ করে) ভিত্তিতে বরাদ্দ করতে হবে। এটি নিষ্ক্রিয় হওয়া উচিত (অতএব স্ক্যানের নাম), কারণ বাহ্যিক ট্র্যাফিক তার আইপি আইডি ক্রমকে ধাক্কা দেবে, স্ক্যানের যুক্তিকে বিভ্রান্ত করবে। আক্রমণকারী এবং জম্বি এবং জম্বি এবং টার্গেটের মধ্যে যত বিলম্ব হবে তত দ্রুত স্ক্যান এগিয়ে যাবে।

যখন একটি পোর্ট খোলা থাকে, আইপিআইডি 2 দ্বারা বৃদ্ধি পায়।

1. টার্গেট করার জন্য আক্রমণকারী -> SYN, জম্বি টার্গেট -> SYN/ACK, জম্বি টার্গেট -> RST (1 দ্বারা আইপিআইডি বৃদ্ধি)
2. এখন আক্রমণকারী ফলাফলের জন্য জম্বি অনুসন্ধান করার চেষ্টা করে। জম্বি আক্রমণকারী -> SYN/ACK, জম্বি থেকে আক্রমণকারী -> RST (1 দ্বারা আইপিআইডি বৃদ্ধি)

সুতরাং, এই প্রক্রিয়ায় আইপিআইডি অবশেষে 2 দ্বারা বৃদ্ধি পায়।

ধন্যবাদ

(THANK YOU)