

স্নিফিং

প্যাকেট স্নিফার একটি প্রোগ্রাম যে তথ্য প্যাকেট থেকে তথ্য প্যাকেট থেকে ধারণ করে।
যেমন- একটি প্যাকেট এর মাধ্যমে ইউজার নেইম আর পাসওয়ার্ড যাচ্ছে তখন প্যাকেট স্নিফার
করে সেই ইউজার নেইম আর পাসওয়ার্ড সংগ্রহ করা যায়।

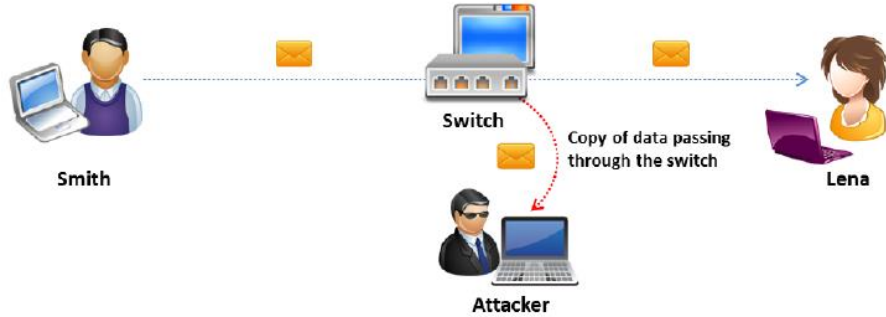
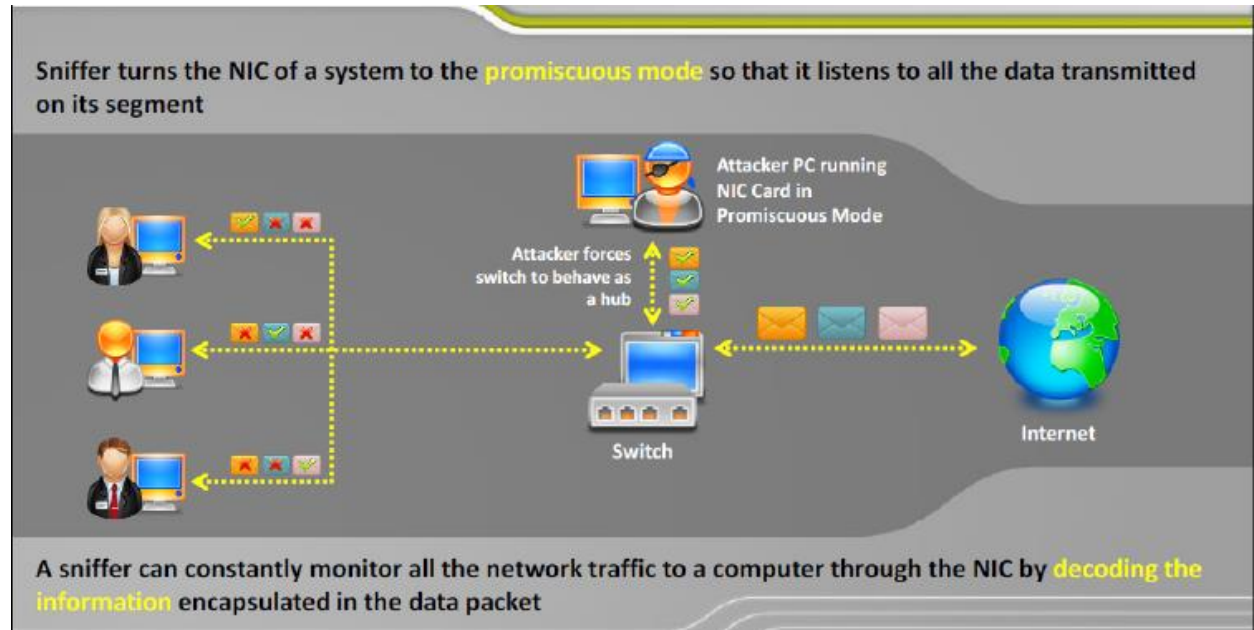


FIGURE 7.1: Packet Sniffing Scenario



স্মিফিং এর প্রকারভেদ

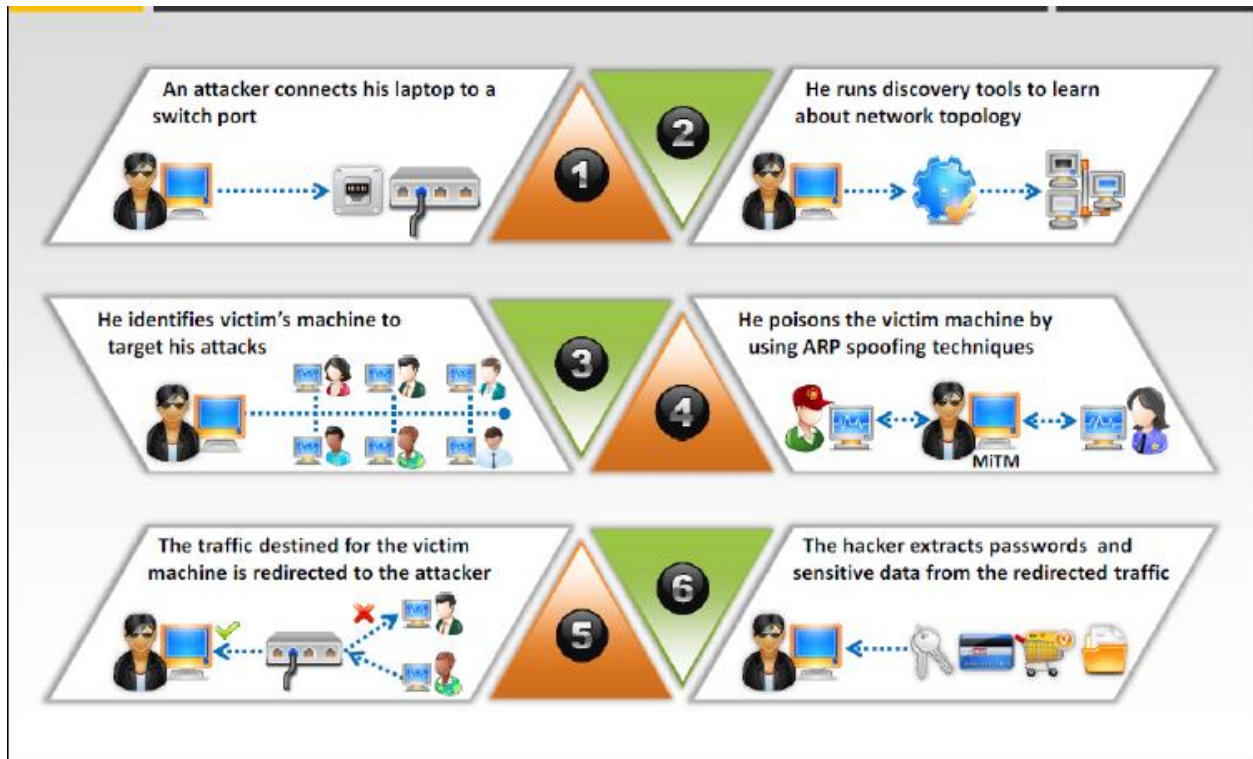
সাধারণত দুই ধরনের স্মিফিং হয়ে থাকে-

১. একটিভ স্মিফিং

২. প্যাসিভ স্মিফিং

একটিভ স্মিফিং

একটিভ স্মিফিং করা হয় সুইচ বেইসড নেটওয়ার্কে। সুইচ ম্যাক এ্যাড্রেস রাখার জন্য একটা ক্যাম টেবিল তৈরি করে। সেই ক্যাম টেবিলে নিজের ম্যাক এ্যাড্রেসকে ইনজেক্ট করে। তারপর এআরপি স্পফিং এর মাধ্যমে ক্যাম টেবিলটি কাস্টম ম্যাক এ্যাড্রেস দিয়ে পরিপূর্ণ করে দেয়। ফলে সুইচটি তখন হাবের মতো করা করা শুরু করে। এবং রিডাইরেক্ট করে দেয় হ্যাকার এর পিসিতে।



প্যাসিভ স্নিফিং

প্যাসিভ স্নিফিং সাধারণত করা যায় যে নেটওয়ার্কে হাব ব্যবহার করা হয়। কারণ হাব সকল পোর্টে ডাটা সেন্ড করে। ফলে খুব সহজেই ডাটা সংগ্রহ করা যায়।

টুলস

Cain and Abel

Winarpattacker


কিভাবে স্নিফিং থেকে সিস্টেমকে রক্ষা করা যায়?

১. আইপি এবং ম্যাক বাইন্ডিং নেটওয়ার্ক সেটআপ করতে হবে।


২. প্লেইন টেক্সট এর পরিবর্তে এনক্রিপ্ট সার্ভিস ব্যবহার করতে হবে।


৩. এইচটিটিপি এর পরিবর্তে এইচটিটিপিএস ও এফটিপি এর পরিবর্তে এসএফটিপি ব্যবহার করতে হবে।

৪. কোন ল্যানকার্ড প্রমিসকাউস মোডে রান হচ্ছে কি না ডিটেক্ট করার জন্য টুল ব্যবহার করা যেতে পারে। যেমন-NMAP



Promiscuous Detection Tool: Nmap





- Nmap's NSE script allows you to check if a target on a local Ethernet has its network card in **promiscuous** mode
- Command to detect NIC in promiscuous mode:**
`nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]`

