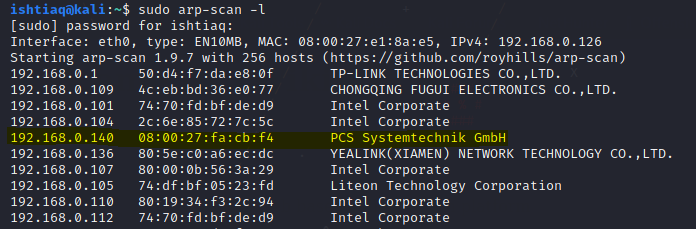
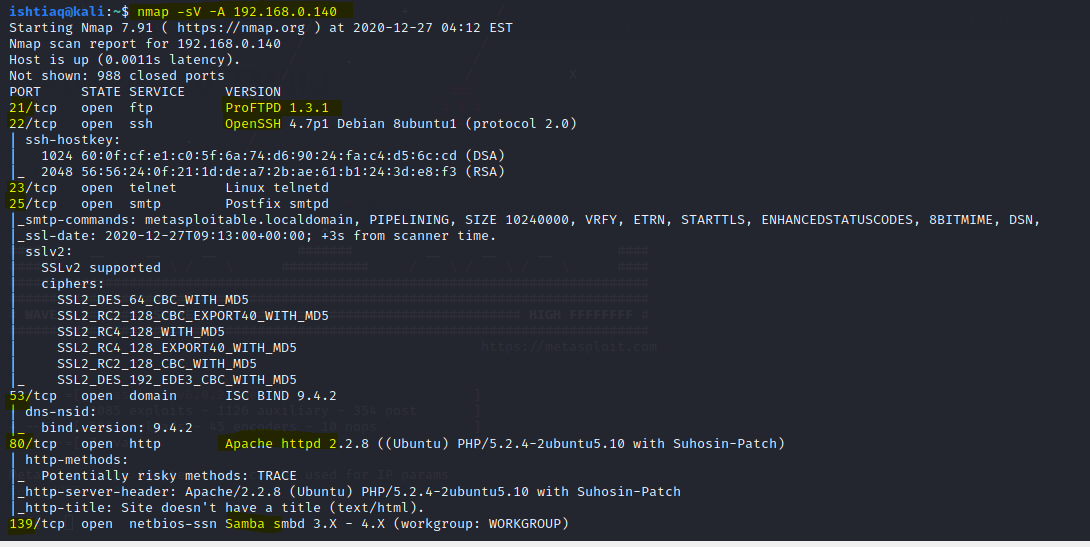
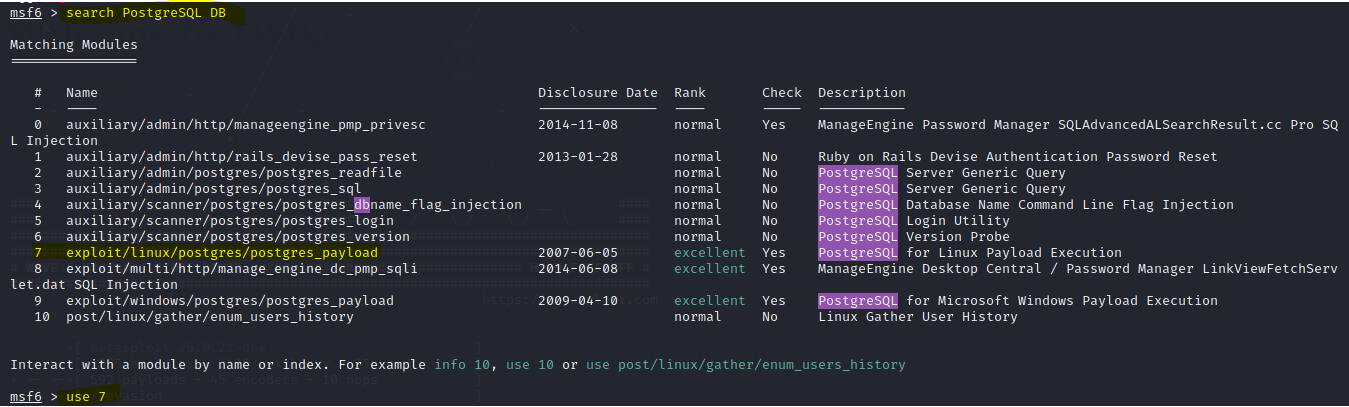
১। প্রথমে আমরা “sudo arp-scan -l” এই কমান্ডটি চালাবো আমাদের আইপি খুজে বের করার জন্য । আমাদের pcs systemtechnik GmbH হচ্ছে আমাদের মেশিন।



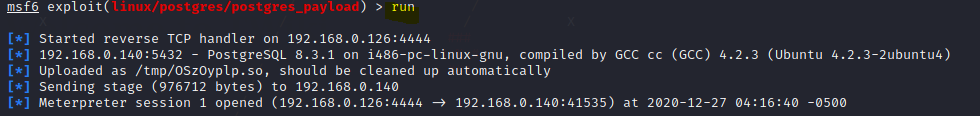
২। এরপর আমরা উক্ত আইপিকে nmap দ্বারা স্ক্যন করব এবং “ nmap -sV -A 192.168.0.140” এই কমান্ডটি চালানোর পর আমরা পোর্টগুলো অবস্থান এবং সার্ভিস সম্পর্কে জানতে পারতেছি।



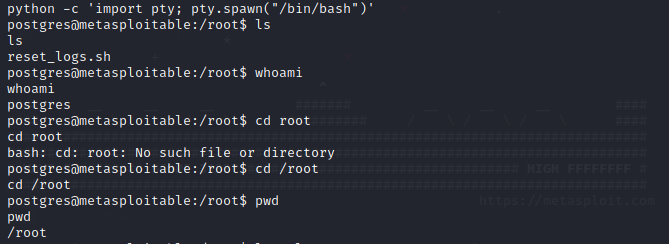
৩। এরপর আমরা সার্ভিস এবং উক্ত পোর্টগুলোর উপর metaexploit চালাবো।প্রথমে আমরা PostgreSQL দ্বারা সার্চ করে পোর্ট নম্বর ৫৪৩২ এইটাতে চালাবো।



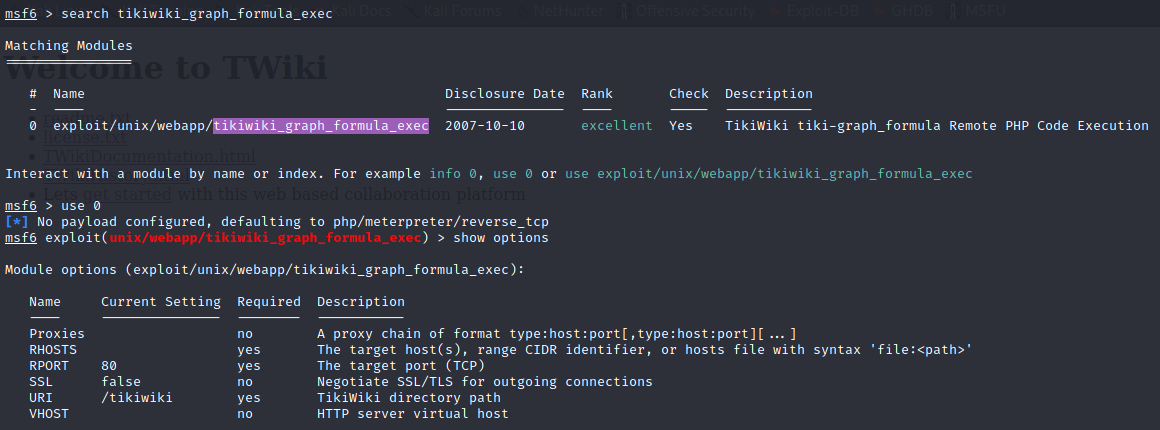
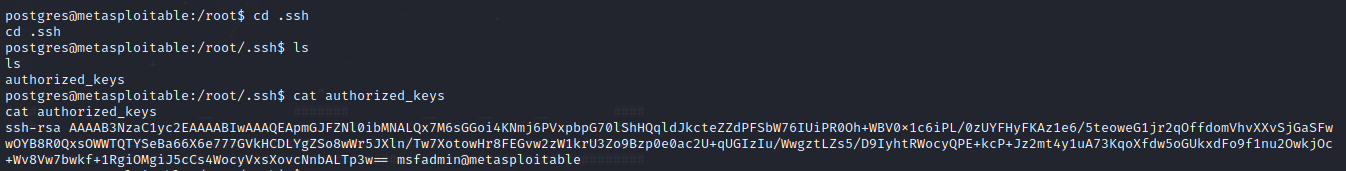
৪। এরপর আমরা RHOST,RPORT এগুলা configure করব।



৫। সুতরাং আমরা মেশিনটিকে compromise করলাম PostgreSQL (৫৪৩২) এই exploit এর মাধ্যমে।



৬। আমরা আরো কয়েকটি মাধ্যমে মেশিনটিকে compromise করতে পারি তার মধ্যে হলো।



ফাইনালি আমরা রুটে ঢুকতে পেরেছি এই exploit গুলোর মাধ্যমে এবং আরো কিছু exploit এর মাধ্যমে করেছি।