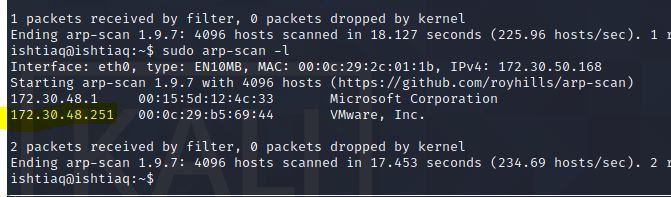
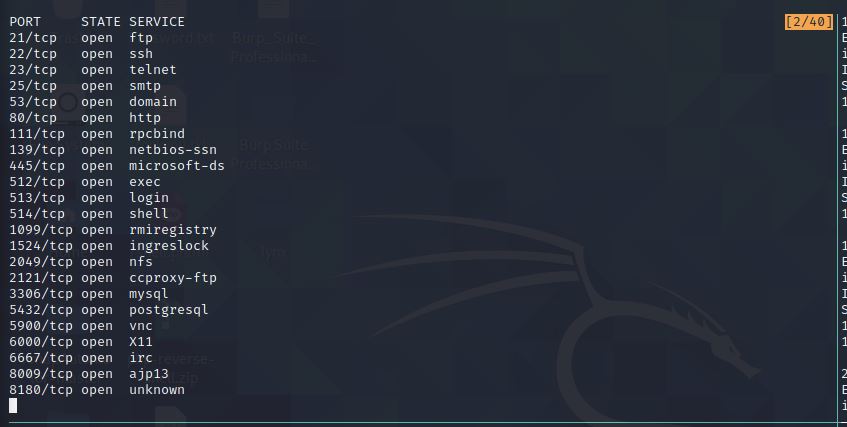
**Metaexploitable 2- Vulnhub Walkthrough**

১। আমি প্রথমে আমার টার্গেট মেশিনকে bridge নেটওয়ার্কে রেখেছি।এরপর এই মেশিনের আইপি খুজে বের করার জন্য “sudo arp-scan -l” এই কমান্ডটি চালাবো।

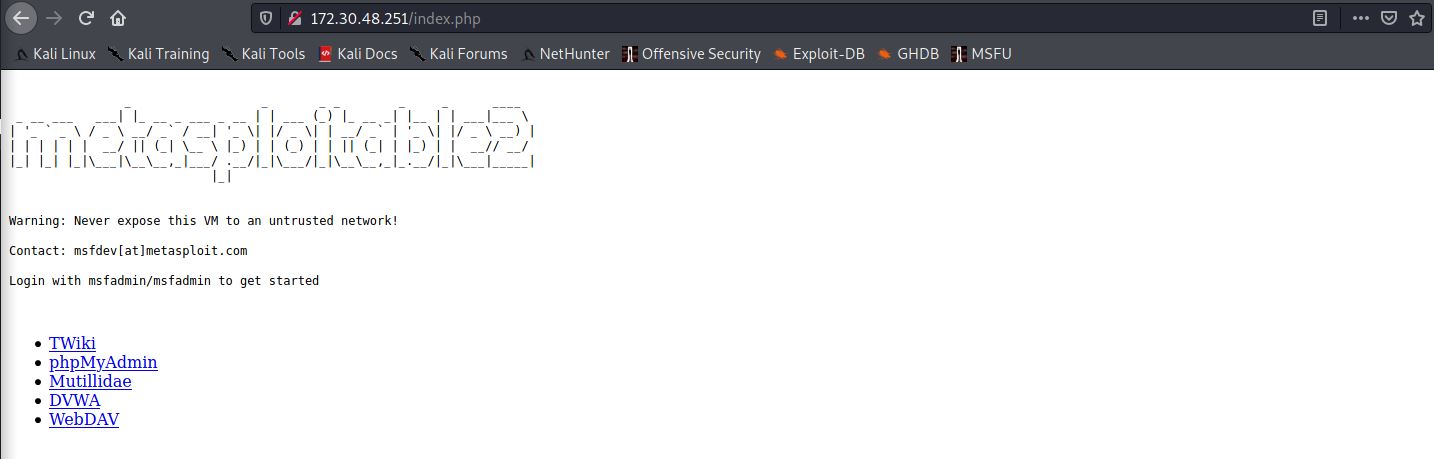


আমরা আমাদের আইপি খুজে পেয়েছি।যেহেতু আমি vmware pro workstation এ ইমপোর্ট করেছি তাই আমার মেশিনটি VMware,Inc হিসেবে দেখাচ্ছে।

২। এরপর আমরা উক্ত আইপির উপর nmap চালাবো তার জন্য কমান্ডটি হলো “nmap 192.168.0.192” এবং আমরা এই পোর্টগুলো ওপেন পাচ্ছি।

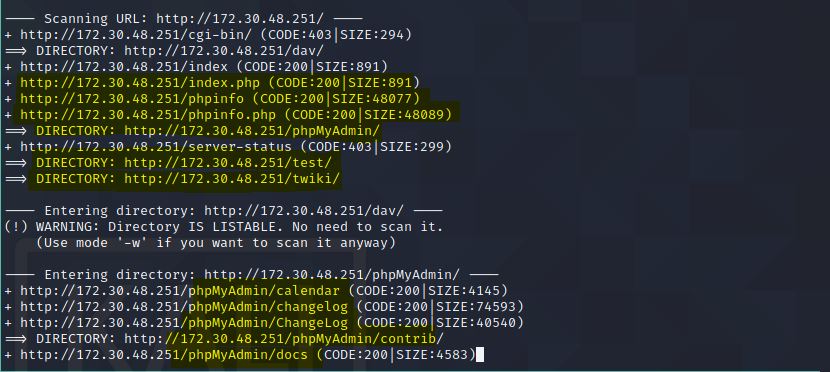


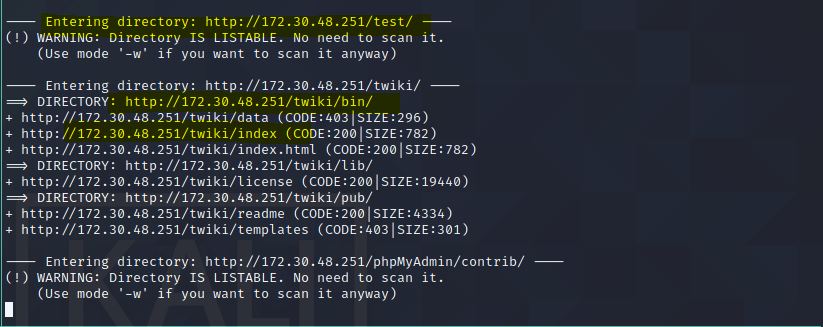
৩। যেহেতু আমরা দেখতে পাচ্ছি ৮০ নম্বর পোর্ট খোলা আছে তাই এটা একটা ওয়েব ব্রাউসার তাই আমরা ব্রাউসারে সার্চ করব উক্ত আইপি লিখে।



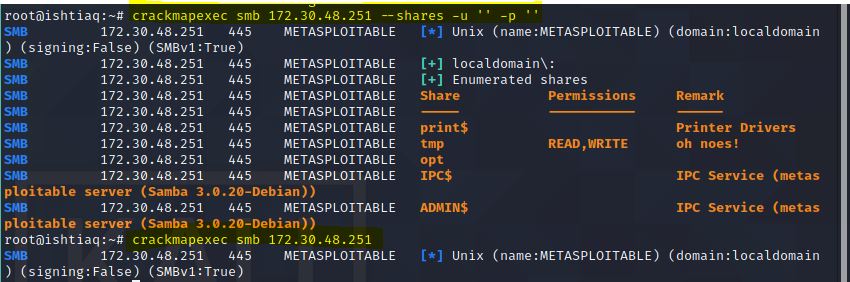
৪। এখন আমরা কি কি ডিরেক্টরি আছে তা দেখব dirb এর মাধ্যমে তার জন্য কমান্ডটি হলো “dirb <http://192.168.0.192>” ।



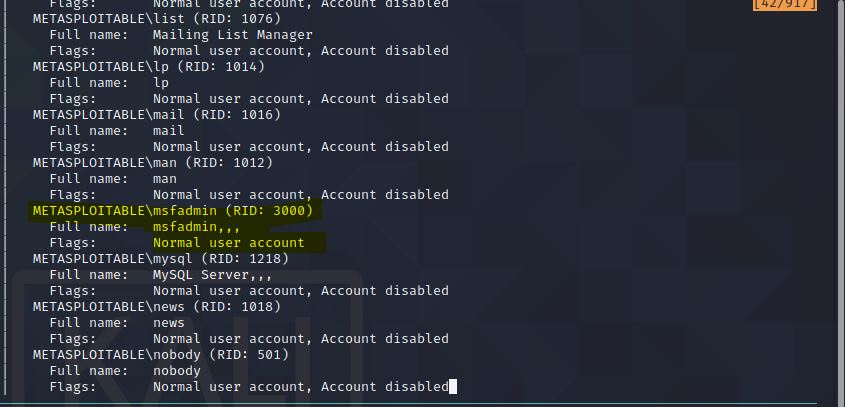




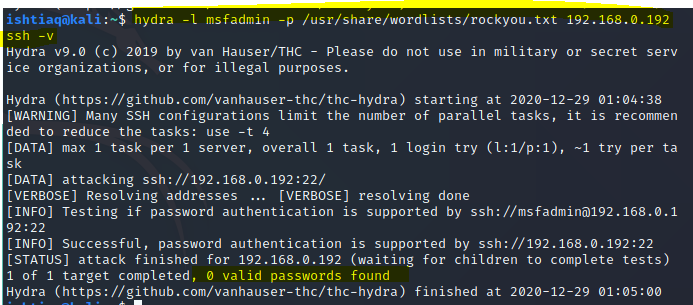
৫। আমরা যখন nmap চালিয়েছিলাম তখন দেখলাম আমাদের smb সার্ভিসটি চালু তাই আমরা এখন আরেকটি কমান্ড চালাবো সেই কমান্ডটি হলো “ **crackmapexec smb 192.168.0.192 --shares -u ‘ ‘ -p ‘ ‘** “ আশানুরুপ কিছু পেলাম নাহ।

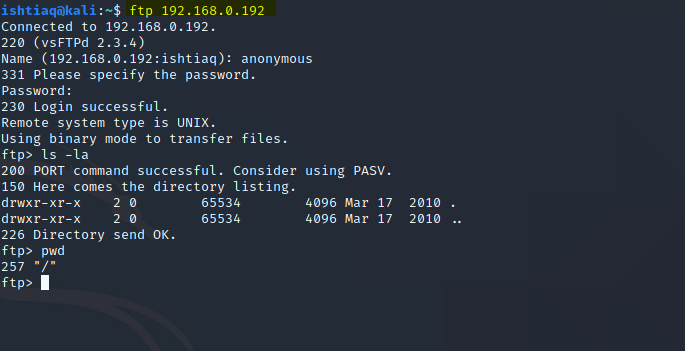


৬। এরপর smb user খুজার জন্য আমরা এই কমান্ডটি চালাবো তাহলো “nmap -sC –script=smb-enum-users 192.168.0.192”

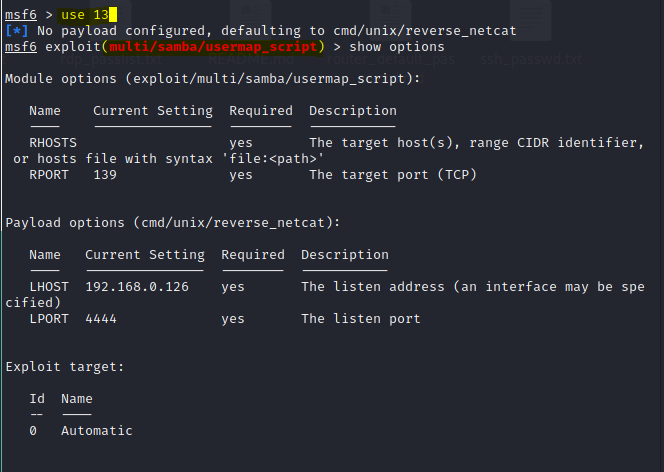


৭। এরপর আমরা “msfadmin” username এরজন্য brute force attack চালাবো এরজন্য কমান্ডটি হলো “hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt -f 192.168.0.192 -s 445 smb”

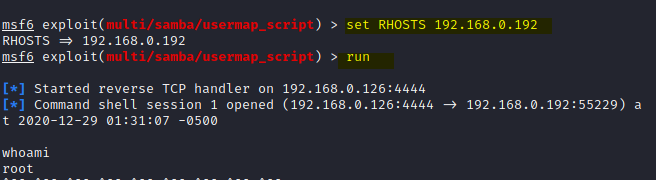


৮। আমরা ftp পোর্ট এ anonymous দিয়ে লগিন করতে পারব। 

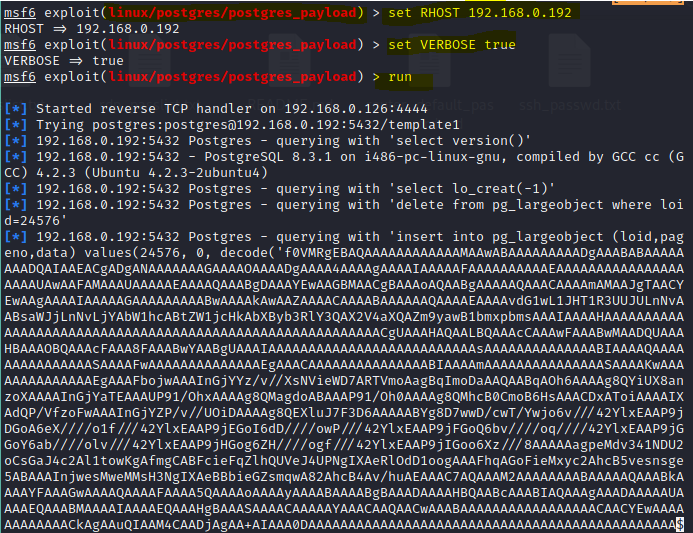
৯। এরপর আমরা Metasploit চালাবো উক্ত 139 পোর্ট এর জন্য exploit চালাবো তার জন্য প্রথমে msfconsole এ যাব এরপর আমরা “samba/usermap\_script” সার্চ করব এবং RHOSTS,Payload সেট করব।



এরপর আমরা exploit অথবা run লিখে ইন্টার প্রেস করব এবং এই মেশিনের জন্য এই exploit টি কাজ করেছে।



১০। আমরা আরো অনেকগুলো exploit চালাতে পারব এবং আমি আরেকটি পোর্ট এ attack করেছিলাম সেটাও দেখাচ্ছি তা হল-



এখন নিজেরা বাকি পোর্টগুলো তে exploit করার ট্রাই করেন।