Using a Database

* Figure out how to send the list of open ports you get from nmap to a database

Password sniffing

* Download psnuffle
* Run it
* Feed psnuffle a pcap file to search for passwords in

SMB

* determine what named pipes are available over SMB
* will running the scanner without credentials return a great deal of information? Why/why not
* use the pipe\_dcerpc\_auditor scanner
* scan the VM and determine if it supports *SMB2* protocol
* list any SMB shares that are available the VM
* ust the smb\_login module to attempt to login to SMB
* determine what local users exist the system using smb\_lookupsid
* determines the version of the SMB service that is running using smb\_version

Idle Scanning

* use scanner/ip/ipidseq to determine which hosts are idle on the network (if there are none, create another account on the metasploitable2 VM, idle, and try again)
* scan the idle VM and determine why scanning an idle machine is the most effective method

dcerpc

* determine what services are available on the VM using the endpoint\_mapper module in metasploit
* find RPC services that aren’t in Endpoint Mapper
* scan a range of IP addresses and obtain info from the Remote Management interface of the DCERPC service using the dcerpc/management module
* find out what DCERPC services you can use on a TCP port using the dcerpc/tcp\_dcerpc\_auditor module

[optional]SNMP (you will need vyatta to simulate a router that you can launch an SNMP attack on)

* search SNMP, bringing up the *MIB (***Management Information Base***) API.* From there, run snmp\_enum