Lesson Plan  
Nmap

short line

# Summary

1. Goals
2. Preparation
3. What is Reconnaissance?
4. CTF

# Goals

* Learn about Forward Shell & Reverse Shell
* Exploit some systems with reverse shell & forward shell
* Understand in network layer how this works

# Preparation

* Kali VM
* Openvpn config file ready to log in to vpn server

# What is Reconnaissance?

* The word *reconnaissance* is borrowed from its military use, where it refers to a mission into enemy territory to obtain information. In a computer security context, reconnaissance is usually a preliminary step toward a further attack seeking to exploit the target system. The attacker often uses [port scanning](https://searchmidmarketsecurity.techtarget.com/definition/port-scan), for example, to discover any vulnerable [ports](https://searchnetworking.techtarget.com/definition/port). After a port scan, an attacker usually exploits known vulnerabilities of services associated with open ports that were detected. (<https://whatis.techtarget.com/definition/active-reconnaissance>)

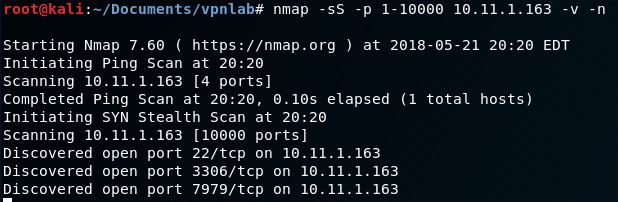
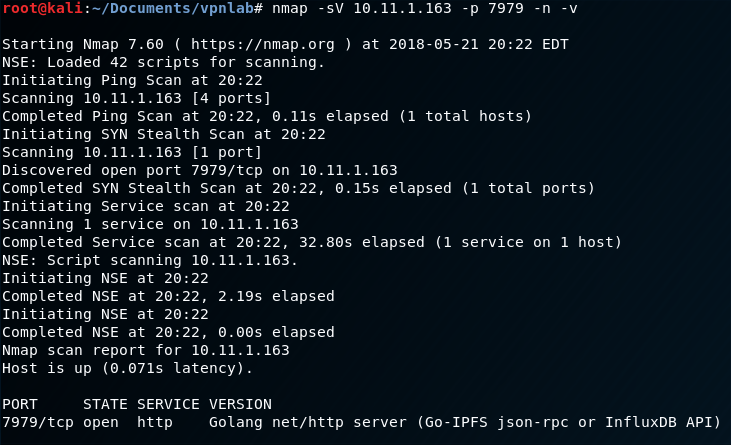
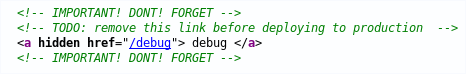
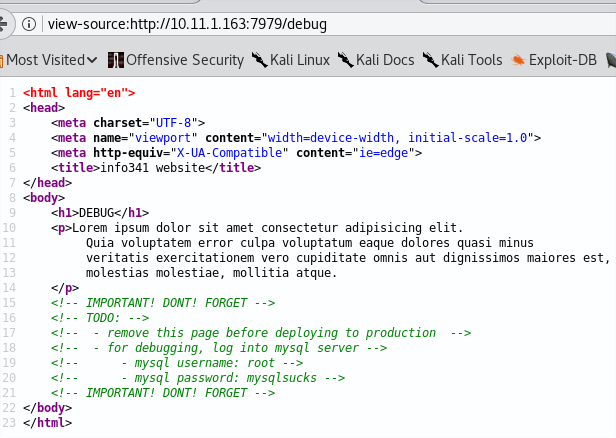
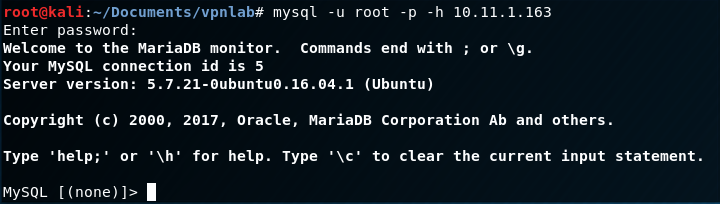
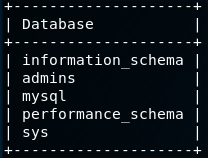
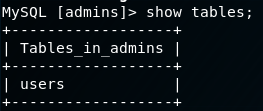
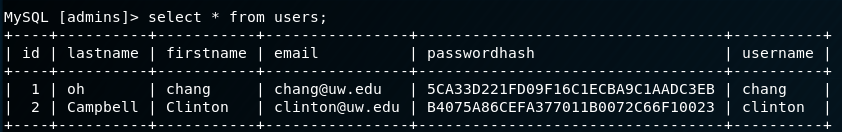
# Lab

* Log into VPN server with Openvpn with your Kali VM as your attacking machine
* Target IP: 10.11.1.163
* Scenario: there is a web server running in a port under 10000. Use nmap to find the web server, and see if you can find the flag in this system.

Tip: https://hashkiller.co.uk/md5-decrypter.aspx

# SPOILER ALERT!

# ====================ANSWER========================

* Start with nmap scan of the target IP from port 1-10000
* 
* We immediately notice that there is a suspicious port running some service in port 7979.
* Also note that mysql is probably running on port 3306
* Using nmap’s Version Scan, we can check which service is running on this port
* 
* Checking the web server on 7979, look for clues that could give us a shell or some sort of credentials.
* First, check the source of html page, and see if there’s any development comments left over.
* Aha!
  + 
* Browse to /debug page and check the source again
  + 
  + This gave us mysql credentials!
  + Let’s log in
* 
* Checking db, there is one db called admin, lets check that out
* 
* 
* There is a table called users
* 
* We found username and password! But password is hashed in what looks like MD5 hash.
  + Let’s see if we can crack it using online md5 crackers.
    - https://hashkiller.co.uk/md5-decrypter.aspx
  + Using the web app, username chang has password: ***P@ssW0rd***
  + Clinton has password: ***whatdoesthefoxsay***
* Using either one of these credentials, log into the machine with ssh
* And the flag is there!