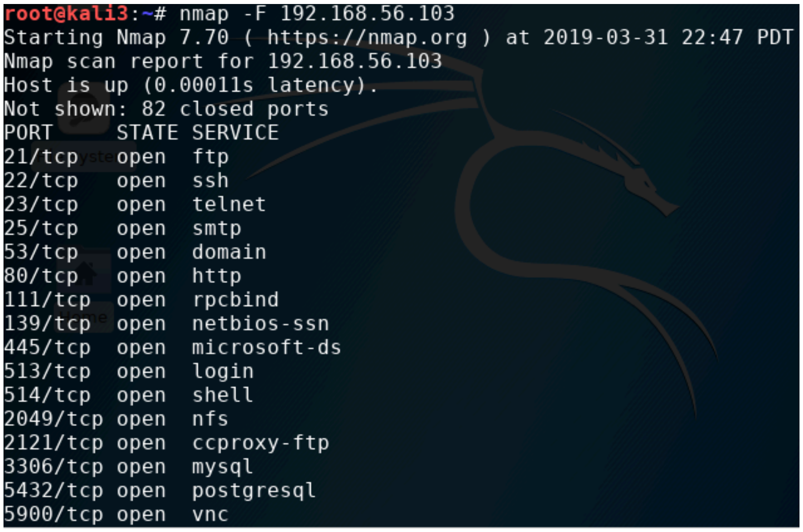
Willis Allstead
3/31/19
CS 445

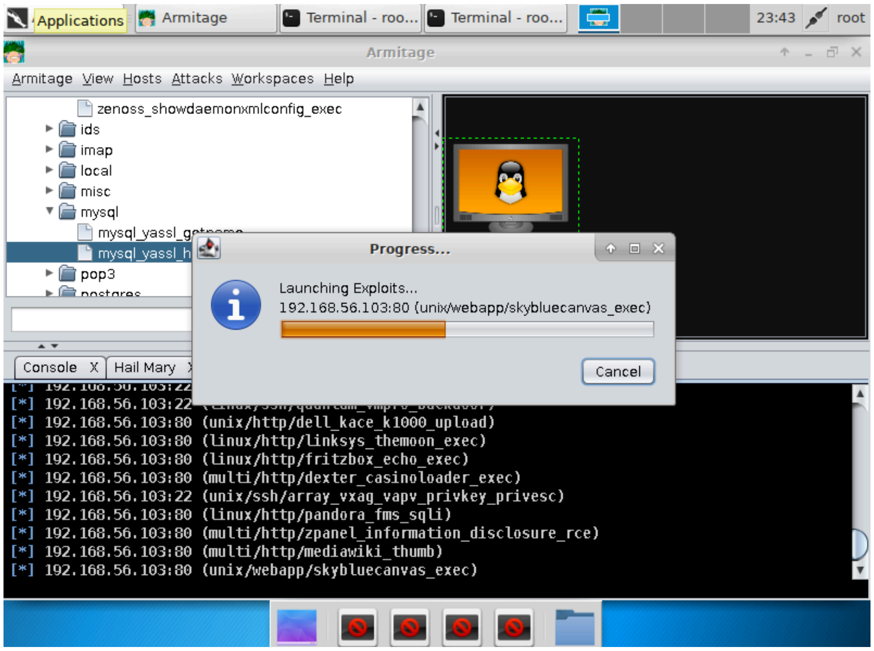
Metasploit



```
root@kali3:~# nmap -F 192.168.56.103
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-31 22:47 PDT
Nmap scan report for 192.168.56.103
Host is up (0.00011s latency).
Not shown: 82 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
```

After installing metasploit on my kali linux light VM and then installing Armitage I could start exploiting my metaexploitable VM. I opened up Armitage, added the metaexplotaible VM as a host and ran a scan on it. The results were the same as I got using nmap above, which makes sense since that program is being used under the hood.

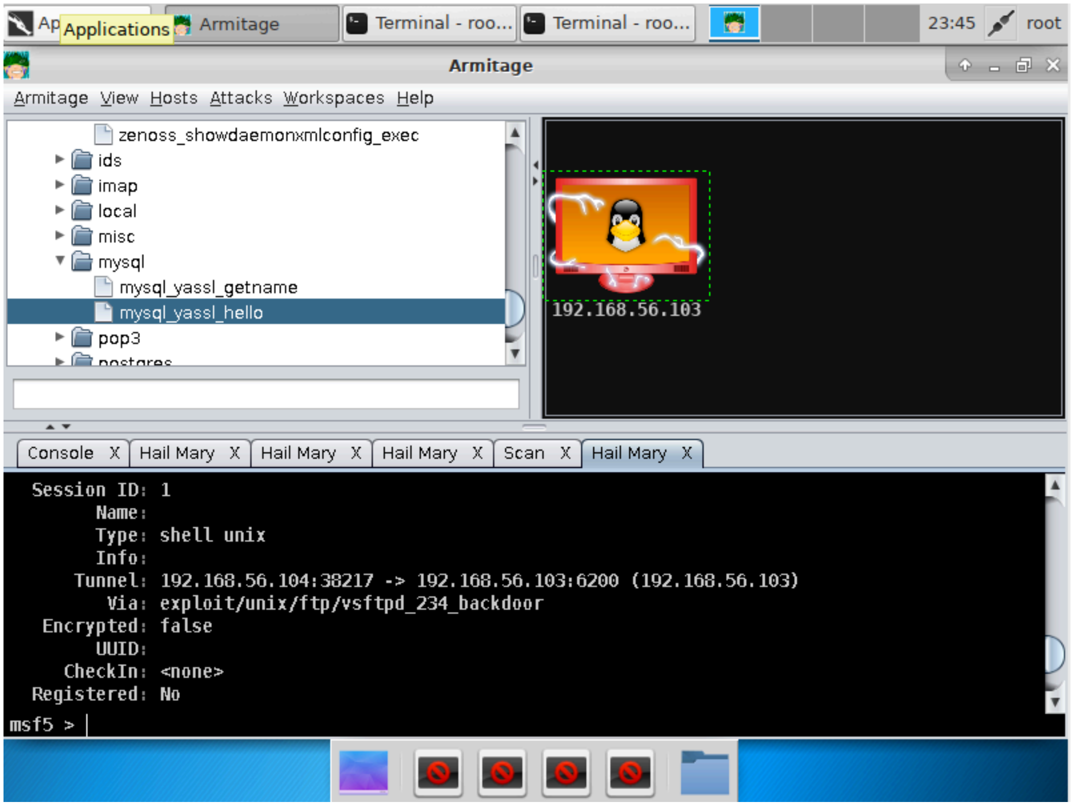
I then ran a "Hail Mary" on the host after specifying the host's OS as Linux.



Launching Exploits...
192.168.56.103:80 (unix/webapp/skybluecanvas_exec)

```
[*] 192.168.56.103:22
[*] 192.168.56.103:80 (unix/http/dell_kace_k1000_upload)
[*] 192.168.56.103:80 (linux/http/linksys_themoon_exec)
[*] 192.168.56.103:80 (linux/http/fritzbox_echo_exec)
[*] 192.168.56.103:80 (multi/http/dexter_casinoloader_exec)
[*] 192.168.56.103:22 (unix/ssh/array_vxag_vapv_privkey_privesc)
[*] 192.168.56.103:80 (linux/http/pandora_fms_sqli)
[*] 192.168.56.103:80 (multi/http/zpanel_information_disclosure_rce)
[*] 192.168.56.103:80 (multi/http/mediawiki_thumb)
[*] 192.168.56.103:80 (unix/webapp/skybluecanvas_exec)
```

After the hail mary finished, there were 5 successful shell sessions started. Here is one that was started using an ftp daemon backdoor. All of these shells could be used to further exploit a host.



```
 Session ID: 1
       Name:
       Type: shell unix
       Info:
     Tunnel: 192.168.56.104:38217 -> 192.168.56.103:6200 (192.168.56.103)
        Via: exploit/unix/ftp/vsftpd_234_backdoor
  Encrypted: false
       UUID:
    CheckIn: <none>
 Registered: No
msf5 >
```