



Recon and Intro to Kali Linux

Session 4



Slides:

<https://tinyurl.com/y9xvh96j>

Announcement:

CTF Nights!



Recap: How to Hack a Website

- Common exploits
 - SQL Injection
 - XSS
 - Session Hijacking and CSRF
- **Scanning**
- Gaining Access
- Maintaining Access
- Covering Tracks



So... What's Reconnaissance? Why do we do it?

- Basically: gaining information about the target - scoping out their vulnerabilities
- Usually, up to 3/4ths of a hack is spent doing recon!
- Narrow down to specific targets and techniques
- Avoid broad scans
- Identify brands/versions to target vulnerabilities
 - **Operating System**
 - **Patch Level**



**We do recon to narrow
down our search, and save
time during actual
exploitation**



Overview

So what do we want to gather?

- IP Address ranges
- Figure out OS
- Port Scanning

IP Address

- A number that identifies your computer on the internet!
- Every phone, computer, tablet has an Internet Protocol address.
- Can be used to figure out where you're accessing the internet from



View your basic network information and set up connections



Types of Reconnaissance

Passive Reconnaissance

- First/Most basic step
- Indistinguishable from ordinary public traffic
- Google searches
- Browsing company web pages

Active Reconnaissance

- Want to know what kind of servers they're running before doing this
- Network scanning
- Social engineering
- Spear phishing
- Ping sweep: Super noisy/obvious



Demo

Google + whois + Wayback
Machine + Netcraft

- We want to find a point of attack
- Information about:
 - Domain name
 - IP Addresses
 - Employee information
 - Phone numbers
 - E-mails
 - Job Information

Google Hacking/Dorking

Using keywords with Google searches is a great way to find web pages that website owners may not want you to see!

- Finding subdomains of a website: `site:website.com -site:www.website.com`
- Finding admin login pages:
 - `inurl:/admin/login.asp & intext:password`
 - `inurl:login & intitle:Admin Login`
- Other interesting information:
 - `intext:admin & inurl:gov -github & filetype:sql`
 - `inurl:administrators.pwd`
 - Public web cameras: `inurl:"ViewerFrame?Mode=`



inurl:/admin/login.asp & intext:password




Whois

- A Whois query is a database search, to a Whois server on TCP port 43, and it is used to resolve contact information about domain names, IP address blocks, and Autonomous System numbers.
- Can use websites ([like this one](#)) or terminal
- Can be used for websites, or IP addresses
 - whois <IP address/domain name>



Wayback Machine/Netcraft

Search the history of over 445 billion pages on the Internet.



Internet Archive is a non-profit library of millions of free books, movies, software, music, and more.

8.4M 2.1M 2.0M 112K 1.1M 129K 177K

Universal Access to Knowledge **GO**

Advanced Search


Announcements

Pro-Airbnb advertising dominated recent political TV ads in San Francisco

Aaron Swartz Day – Hackathon, Privacy-enabling conference and Reception

Grant to Develop the Next Generation Wayback Machine

[SEE MORE](#)

| | | | | |
|------------------|--|-------------------------|---------------------|--|
| Site | http://sans.org | Netblock Owner | Incapsula Inc | |
| Domain | sans.org | Nameserver | dns21a.sans.org | |
| IP address | 45.60.31.34 (VirusTotal) | DNS admin | hostmaster@sans.org | |
| IPv6 address | Not Present | Reverse DNS | unknown | |
| Domain registrar | plr.org | Nameserver organisation | whols.plr.org | |
| Organisation | The SANS Institute, US | Hosting company | unknown | |
| Top Level Domain | Organization entities (.org) | DNS Security Extensions | unknown | |
| Hosting country |  US | | | |

Hosting History

| Netblock owner | IP address | OS | Web server | Last seen | Refresh |
|--|---------------|-------|------------|-------------|---------|
| Incapsula Inc 3400 Bridge Parkway, Suite 200 Redwood Shores CA US 94065 | 45.60.31.34 | Linux | unknown | 6-Aug-2018 | |
| Incapsula Inc 3400 Bridge Parkway, Suite 200 Redwood Shores CA US 94065 | 45.60.33.34 | Linux | unknown | 22-May-2018 | |
| SANS INSTITUTE 11200 Rockville Pike Suite 200 North Bethesda MD US 20852 | 204.51.94.202 | - | Apache | 28-May-2017 | |
| SANS INSTITUTE 11200 Rockville Pike Suite 200 North Bethesda MD US 20852 | 204.51.94.202 | Linux | Apache | 12-May-2017 | |
| SANS INSTITUTE 11200 Rockville Pike Suite 200 North Bethesda MD US 20852 | 66.35.59.202 | Linux | Apache | 6-Mar-2017 | |
| SANS INSTITUTE 11200 Rockville Pike Suite 200 North Bethesda MD US 20852 | 204.51.94.202 | Linux | Apache | 4-Aug-2016 | |
| SANS INSTITUTE 11200 Rockville Pike Suite 200 North Bethesda MD US 20852 | 66.35.59.202 | Linux | Apache | 22-Jun-2016 | |
| SANS INSTITUTE 11200 Rockville Pike Suite 200 North Bethesda MD US 20852 | 204.51.94.202 | Linux | Apache | 17-May-2016 | |
| SANS INSTITUTE 11200 Rockville Pike Suite 200 North Bethesda MD US 20852 | 66.35.59.202 | Linux | Apache | 16-May-2016 | |
| SANS INSTITUTE 11200 Rockville Pike Suite 200 North Bethesda MD US 20852 | 204.51.94.202 | Linux | Apache | 3-Mar-2016 | |



Summary of techniques from Demo

- **Google Dorking** - find subdomains of website to target and hidden pages
- **Whois** - find information about the registrant of the web application
- **Wayback Machine** - find webpages with useful information from previous versions of a web application
- **Netcraft** - find information about the OS, the IP addresses, the web server and when a security patch may have been last applied



Kahoot Time!



Kali Linux

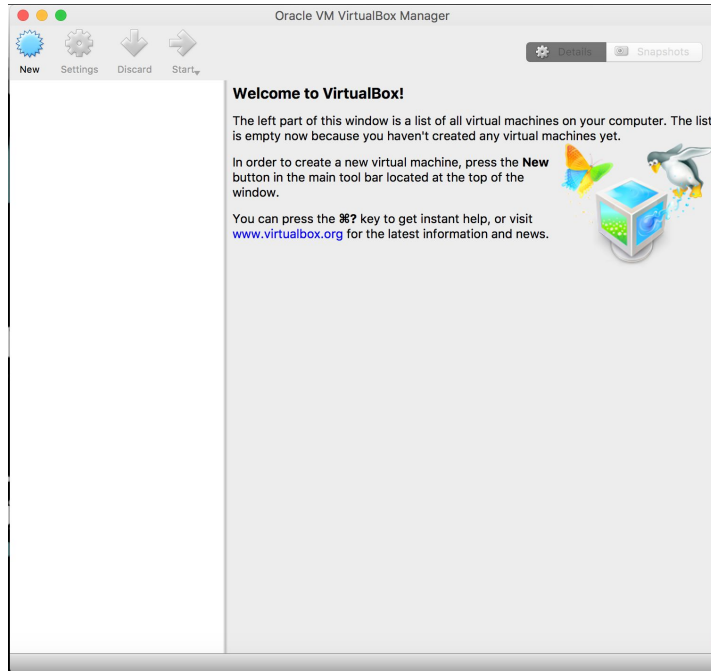


What is Kali?

- ❑ A Linux distribution used primarily by pentesters and security researchers
- ❑ Comes with many pentesting tools out-of-box
- ❑ Information Gathering, Wireless Attacks, Web App Attacks, Password Cracking, Reverse Engineering, Social Engineering



VM Setup

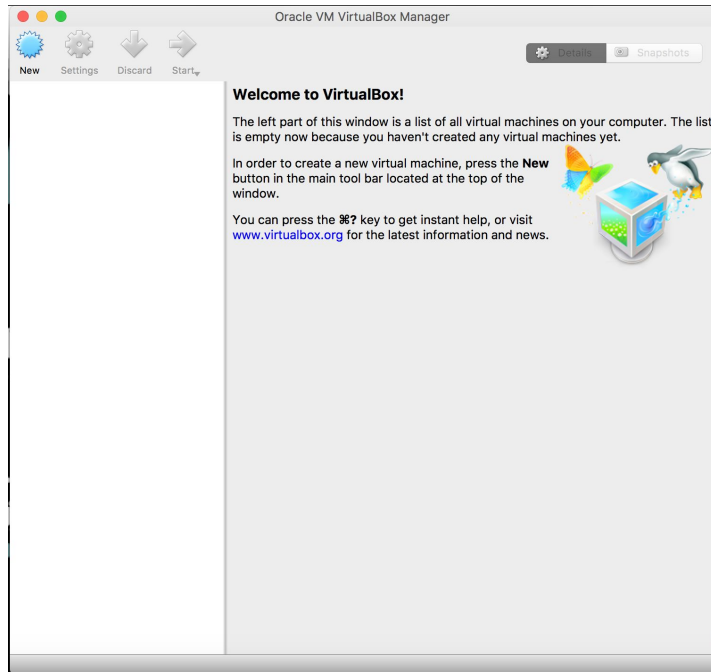


Website

- <https://www.virtualbox.org/wiki/Downloads>



VM Setup



Website

- <https://images.offensive-security.com/virtual-images/kali-linux-2018.4-vbox-amd64.ova>
- Click "VirtualBox Images" and select 64 bit.



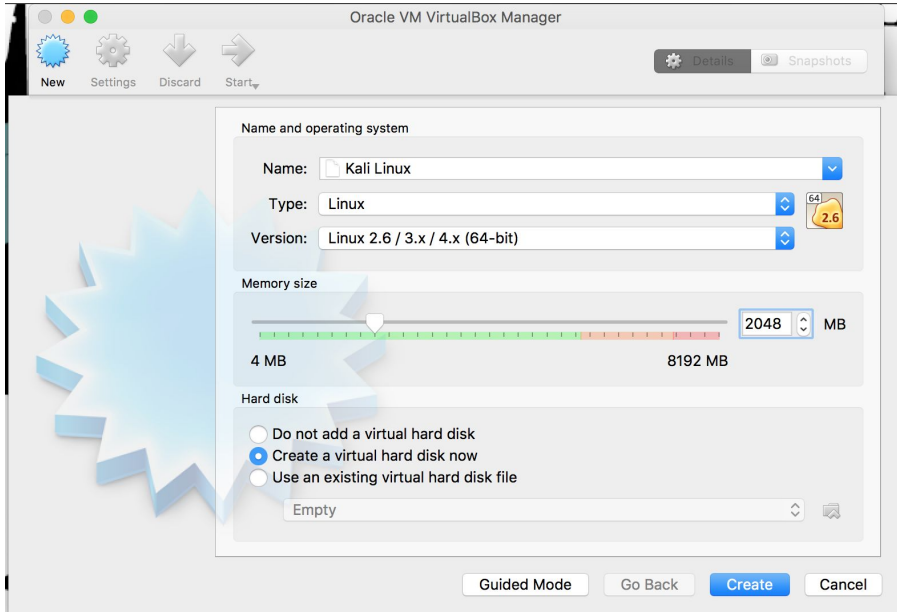
VM Setup

When in doubt - use
the default setting!

Or just ask an officer.



VM Setup

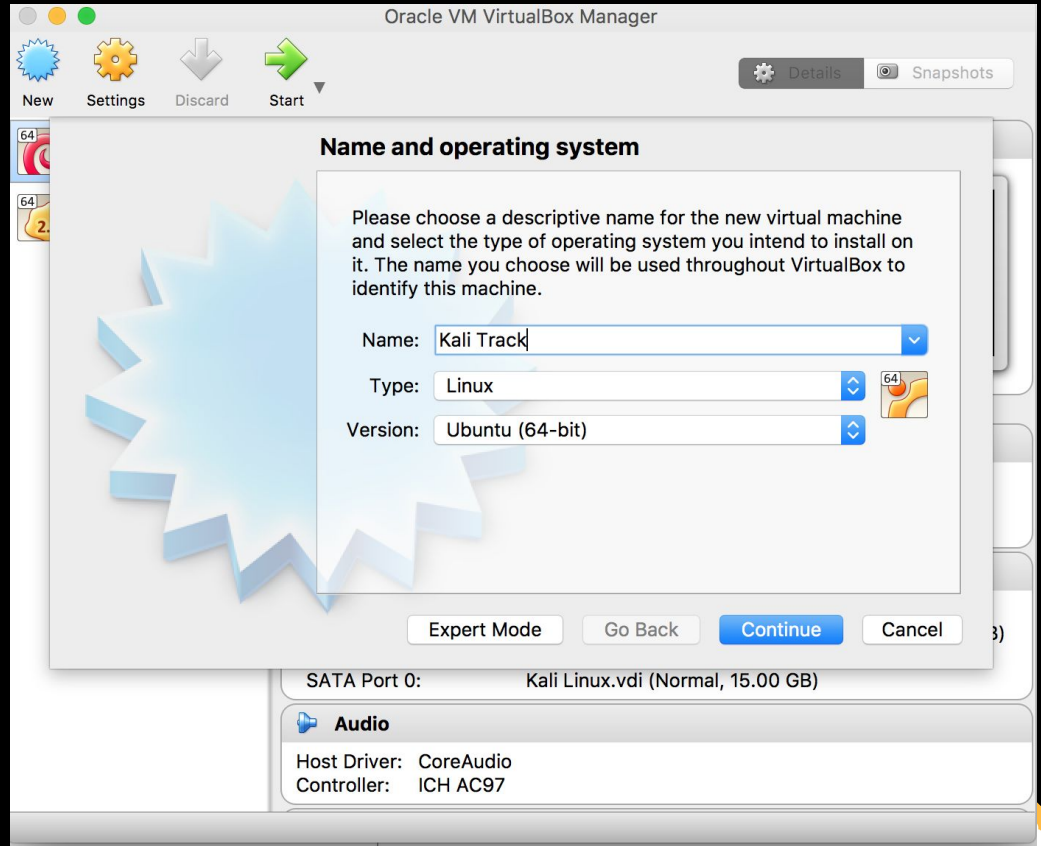


Website

- <https://www.kali.org/downloads/>

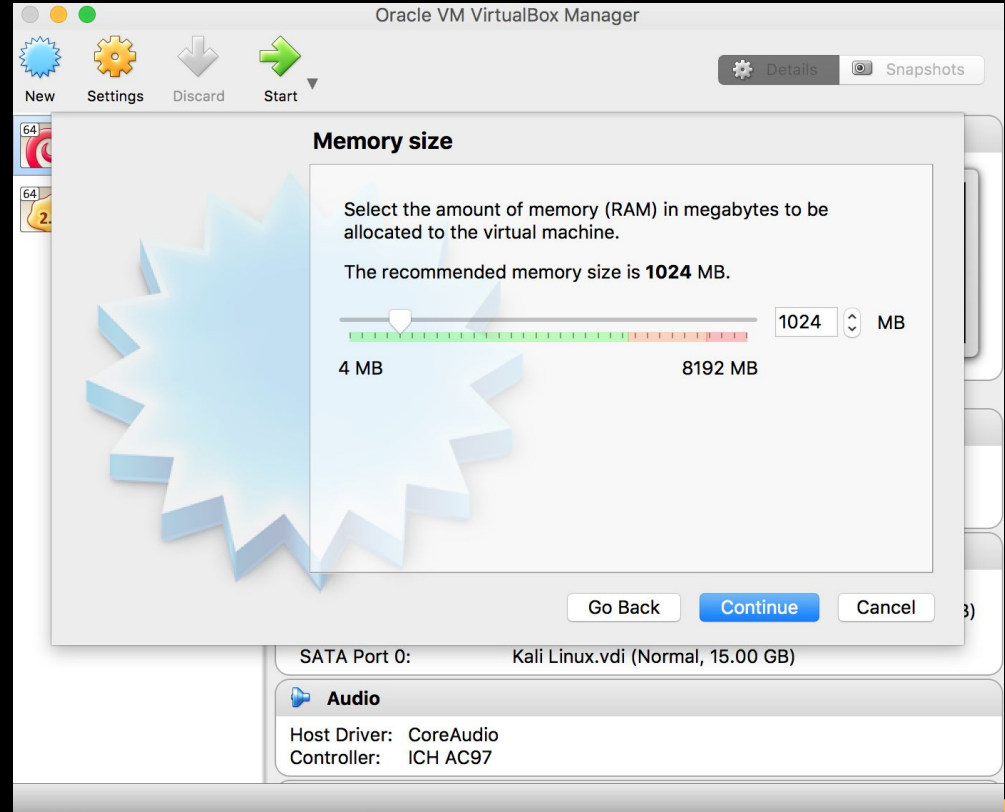


VM Setup

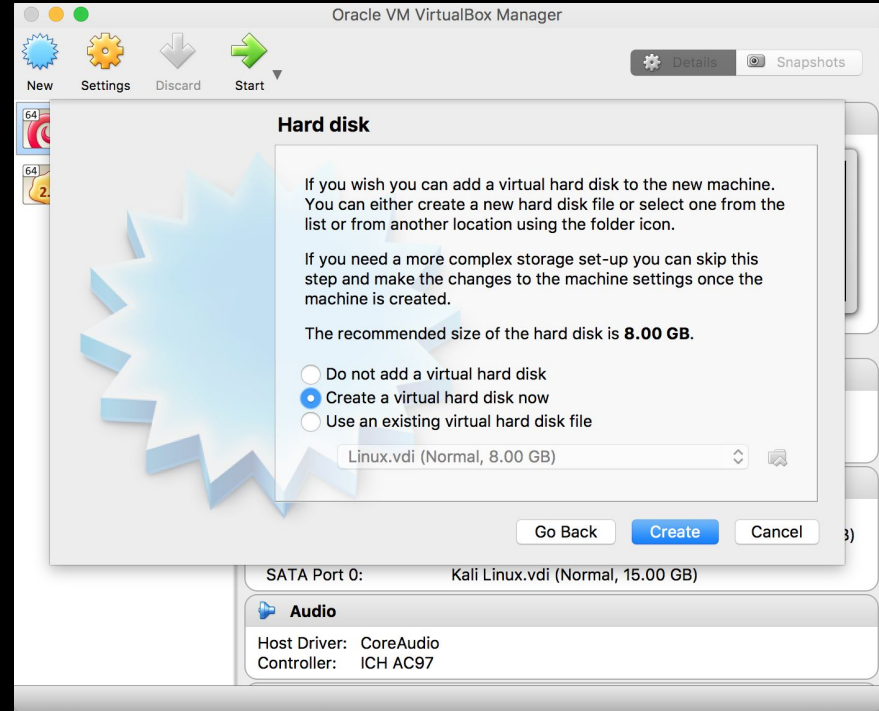


VM Setup

I highly recommend giving up more RAM if your laptop can handle it!



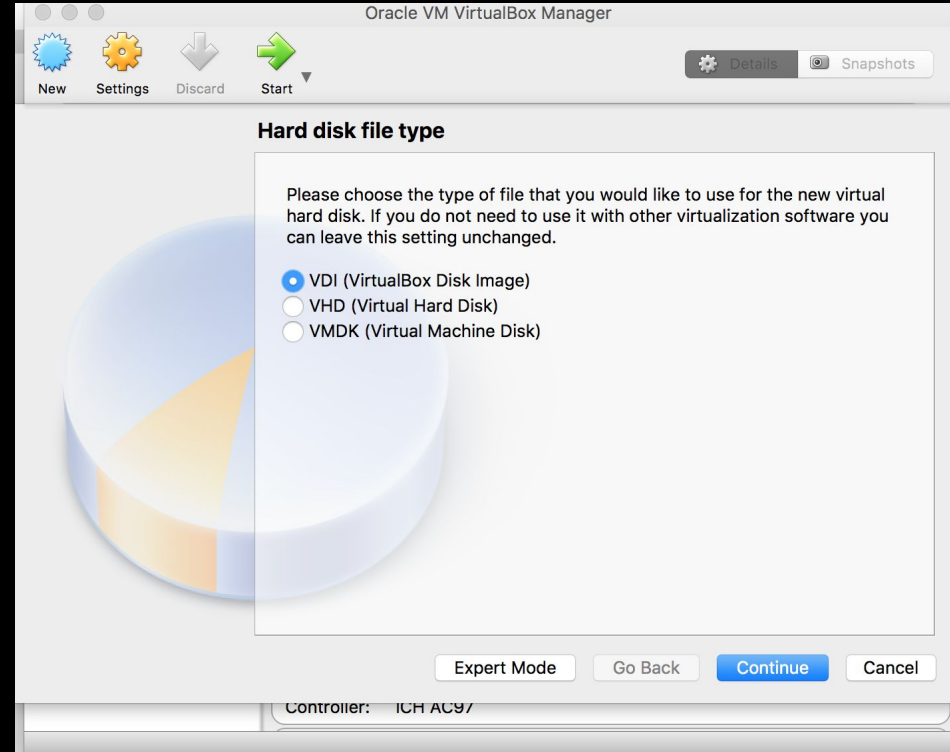
VM Setup



VM Setup

<https://superuser.com/questions/360517/what-disk-image-should-i-use-with-virtualbox-vdi-vmdk-vhd-or-hdd>

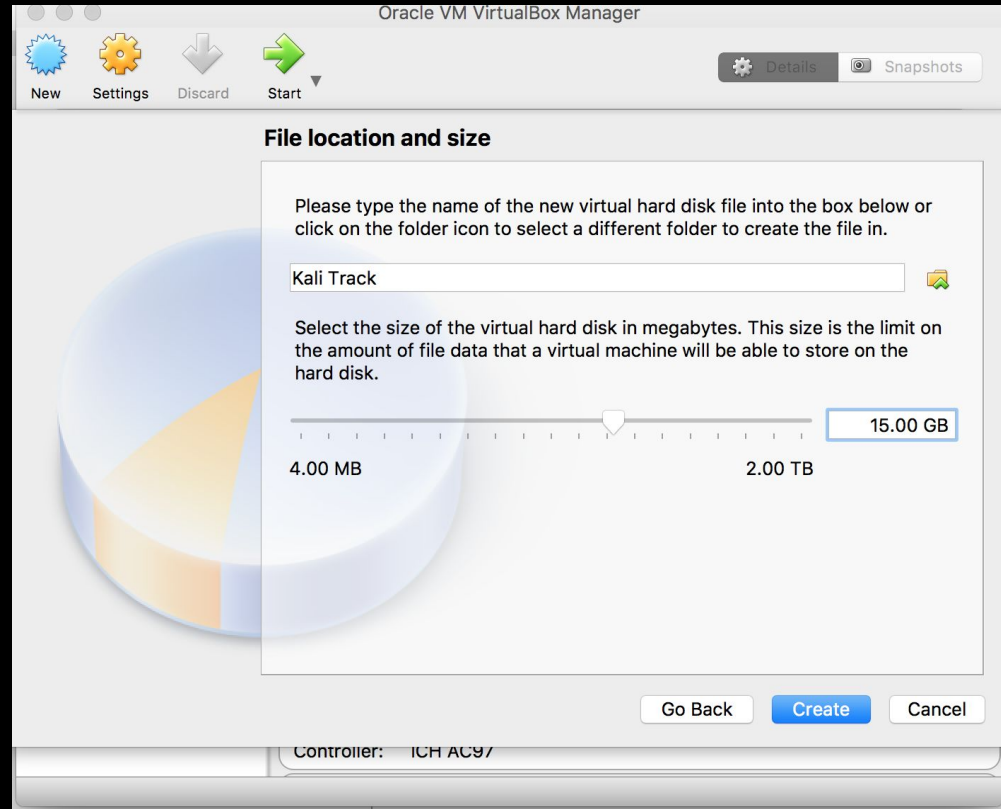
<https://software.grok.lsu.edu/article.aspx?articleid=14214>



VM Setup

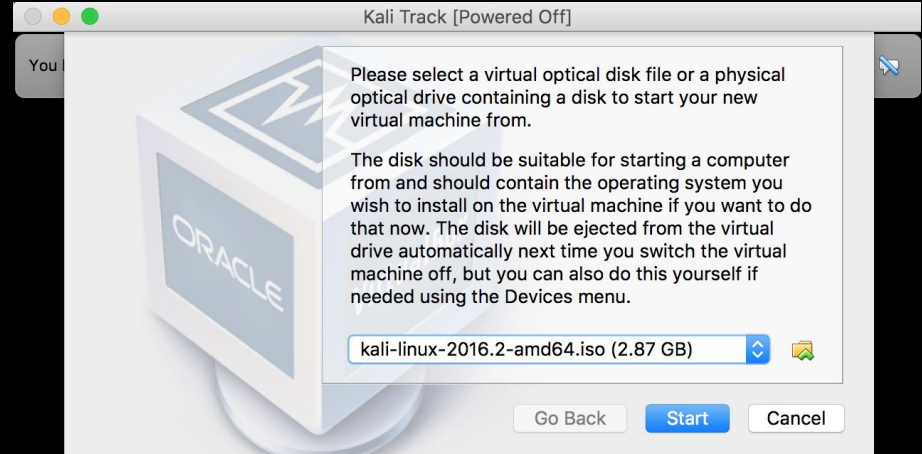


VM Setup



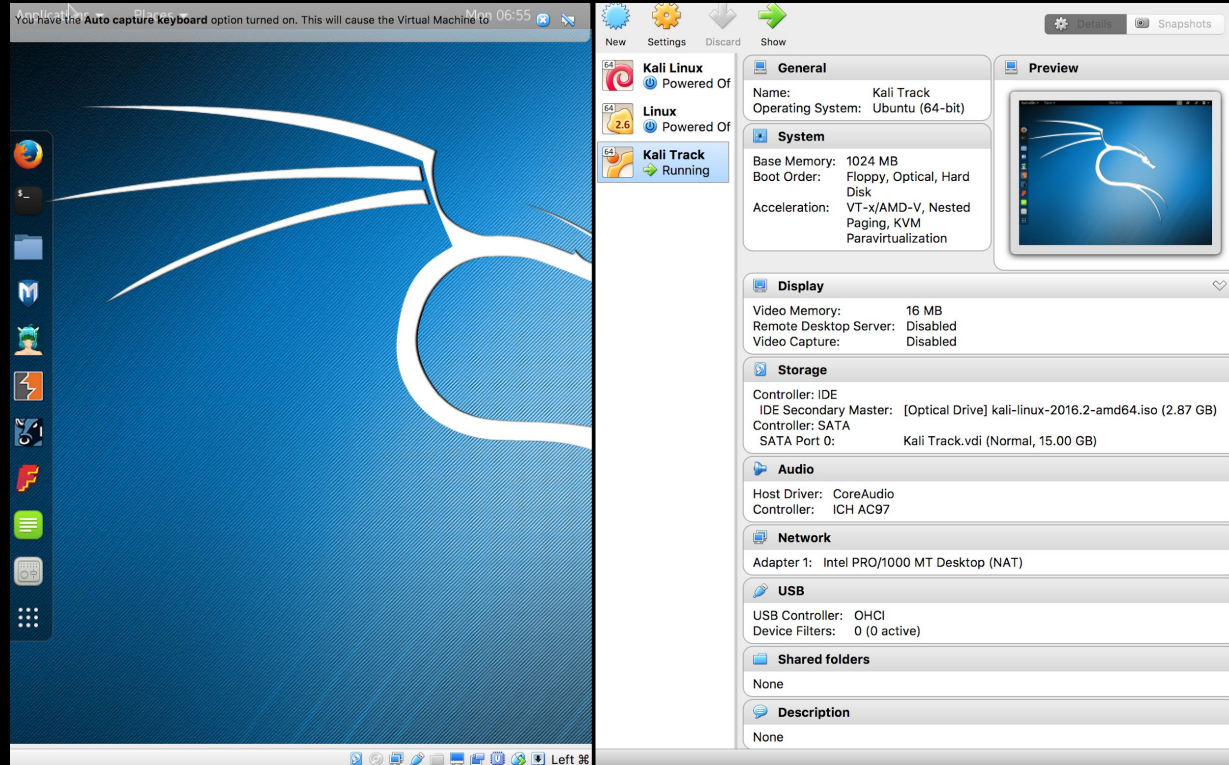
VM Setup

Click the folder icon to select the .iso file where you have the Kali Linux OS downloaded.



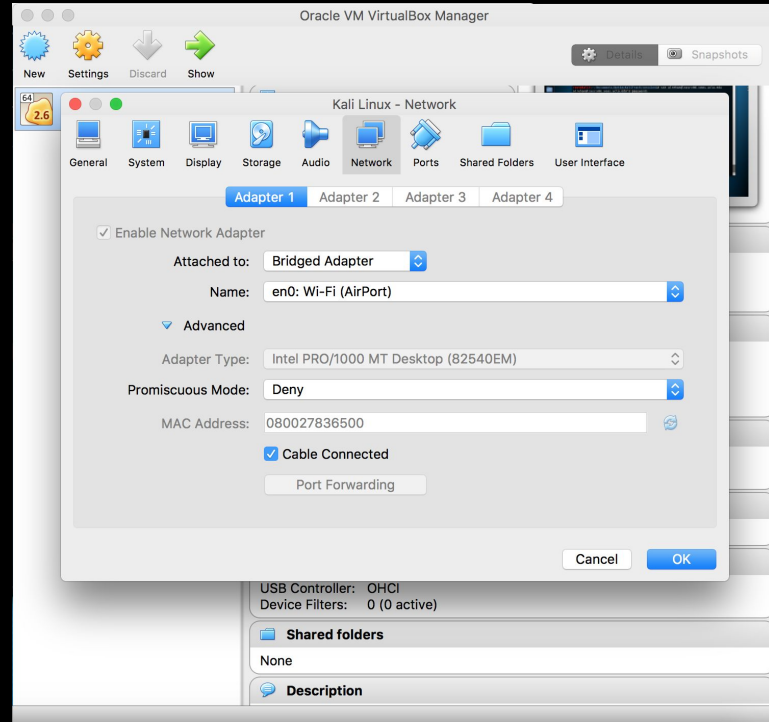
VM Setup

This is my setup, that works fine on my Macbook Pro.



VM Setup

- Make sure you are connected to **eduroam** or **UCLA_WIFI**
- Click on the “Network” header in VirtualBox
- Change “NAT” to “Bridged Adapter” and the name should be “en0”
- Hit “Ok”



password: root
username: toor

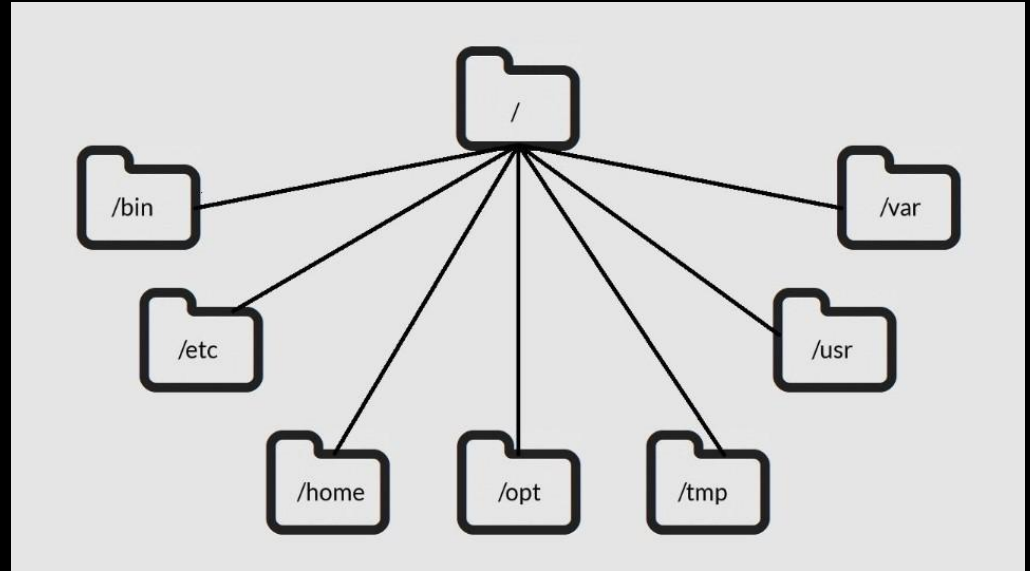


Intro to Linux



Linux File Structure

- Think of Linux as a tree!
- Each folder is a branch and each file is a leaf



Basic Linux Commands

- **pwd** (print working directory)
- **ls** (list files)
- **cat** (print file)
- **cd** (change directory)
- **write** (write ;))
- **who** (who's on the server)
- **mesg** (stop/allow messages)



Linux Command Demo



recon-ng



What it is?

- A Kali Linux tool used to perform web based recon quickly and thoroughly.
- Can use APIs to extract information, if it's given an API key.
 - Eg: Google, Linkedin, Facebook
- Can detect different types of vulnerabilities in a website

This is used for **active** reconnaissance.



Demo

```
shellter
[recon-ng][default] > keys list
```

| Name | Value |
|-------------------|-------|
| bing_api | |
| builtwith_api | |
| facebook_api | |
| facebook_password | |
| facebook_secret | |
| facebook_username | |
| flickr_api | |
| fullcontact_api | |
| google_api | |
| google_cse | |
| instagram_api | |
| instagram_secret | |
| ipinfodb_api | |
| jigsaw_api | |
| jigsaw_password | |
| jigsaw_username | |
| linkedin_api | |
| linkedin_secret | |
| pwnedlist_api | |
| pwnedlist_iv | |
| pwnedlist_secret | |
| shodan_api | |

```
[recon-ng][default][xssposed] > set source sans.org
SOURCE => sans.org
[recon-ng][default][xssposed] > run
```

SANS.ORG

```
[*] Category: XSS
[*] Example: http://www.solidaritepaysans.org/index.php
[*] Host: solidaritepaysans.org
[*] Publish_Date: 2015-09-24 19:28:55
[*] Reference: https://www.xssposed.org/incidents/88650/
[*] Status: unfixed
```

```
[*] Category: XSS
[*] Example: http://www.gameartisans.org/comiconchallenge/2014/index.php#!prettyPhoto/0,%3Cimg%20src=x%20onerror=alert%28/XSSPOSED/%29%3E/
[*] Host: gameartisans.org
[*] Publish_Date: 2015-07-08 14:34:35
[*] Reference: https://www.xssposed.org/incidents/70664/
[*] Status: unfixed
```

SUMMARY

```
[*] 2 total (2 new) vulnerabilities found.
```



Kahoot :)



Thank you!

<https://tinyurl.com/yads4g4g>

