Getting Started with Security

Introduction

What is it?

"Hacking is waking up in the morning, working hard at it until you feel like an idiot, trying over and over, until you solve the problem then going to bed and doing the same thing all over again."

What do I need to start?

- A computer
- Motivation

Mentality

Learning as much as possible.

So where did I start?

- I learned programming at a young age
- Got into making crappy games in Batch
- Wanted to work in game development
- Found out pentesting was a career
- Went to a local meetup
- Watched videos
  - LiveOverflow
- Participated in CTF's

What is the VECC for?

Goals

- Teach you real world skills that you won't learn in your degree
- Cover a range of topics
- Compete in CTF's as a team
- Have fun!

Give a little, take a lot.

We are ready to invest a lot of our time to create resources, challenges and more for you

We need you to commit to spending some of your own time learning the materials

What do you want to learn

There are 4 categories that we *can* teach

- Web Penetration Testing
- Reverse Engineering
- Corporate Penetration Testing
- Network Analysis

Common Content

- Introduction to Linux
- Understanding the web
- How to attack software

CTF's

A CTF is a competition where competitors have to complete challenges

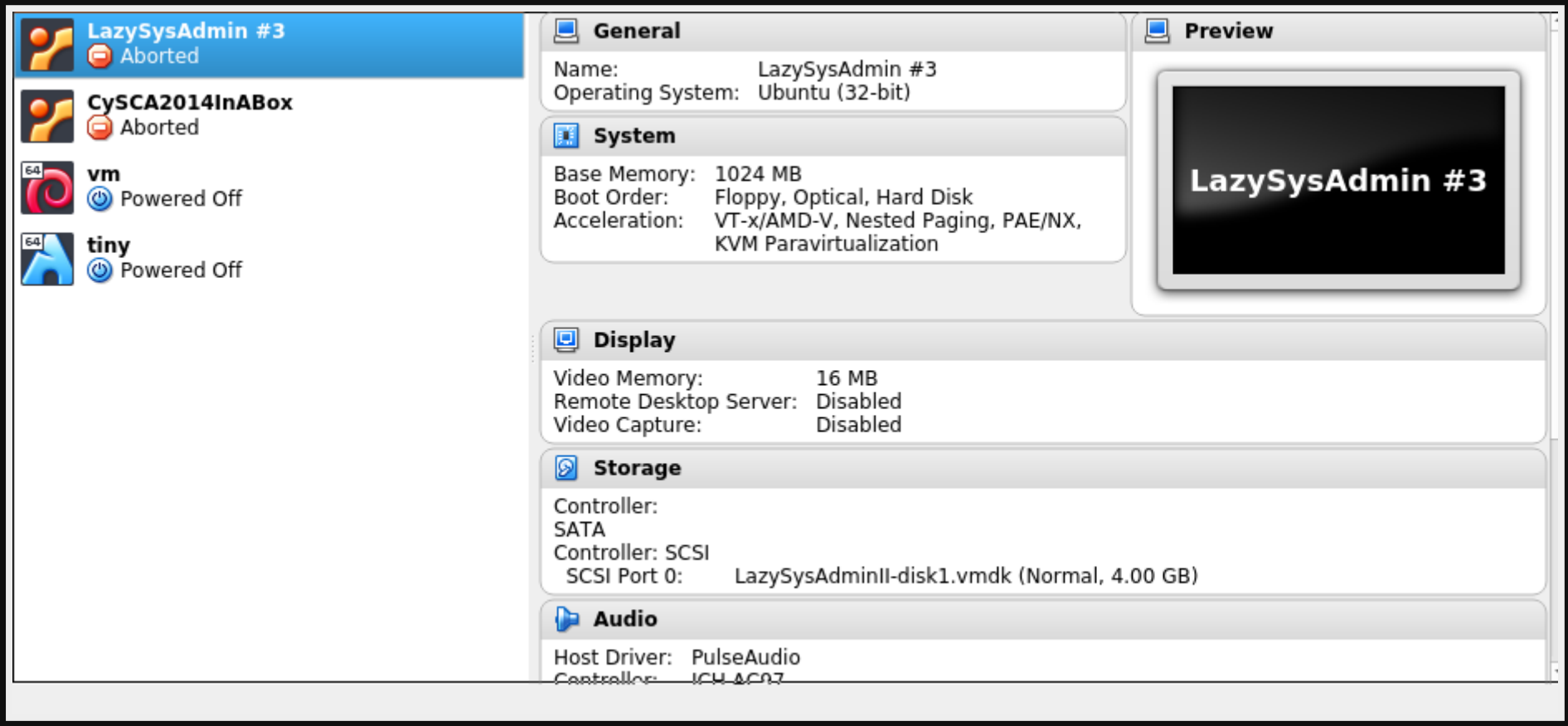
There are two types

- Boot To Root
- Jeopardy Style

Jeopardy Style

- Coding challenges (**17**)
- Cryptography (**26**)
- Forensics (**28**)
- Jail Escaping (**21**)
- JavaScript (**10**)
- Malware Analysis (**17**)
- Pwnage Linux (**19**)
- Reverse Engineering (**44**)

Boot2Root


LazySysAdmin #3
Aborted
CySCA2014InABox
Aborted
vm
Powered Off
tiny
Powered Off
General
Name: LazySysAdmin #3
Operating System: Ubuntu (32-bit)
System
Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization
Preview
LazySysAdmin #3
Display
Video Memory: 16 MB
Remote Desktop Server: Disabled
Video Capture: Disabled
Storage
Controller: SATA
Controller: SCSI
SCSI Port 0: LazySysAdminII-disk1.vmdk (Normal, 4.00 GB)
Audio
Host Driver: PulseAudio

CTF's you can try right now

- PicoCTF (Jeopardy)
- Over The Wire (Jeopardy)
- RingZer0 (Jeopardy)
- VulnHub (Boot2Root's)

Virtualization

Virtualization allows your computer to simulate another fully functioning system.

Choosing the Right Distro

Pre-Built penetration testing

Pros:

- Has everything you need from the get go
- Easy to install

Cons:

- Has a lot of Bloat
- 99% of the tools are useless to you
- You don't learn much Linux

Building up your own

Pros:

- Very little bloat
- Allows you to learn about Linux
- Cool to have your very own setup

Cons:

- Time consuming
- Most tools will have to be compiled from scratch

"Hackerman" Options

- Kali Linux (Easy to set up)
- BlackArch (Moderately hard)
- Arch + BlackArch (Good luck 😁)

Normal options

- Ubuntu
- Mint
- Debian

Options for Virtualization

- VMWare Workstation (Paid, but Free from Uni)
- Oracle VirtualBox (Free)
- Vagrant (Built on VirtualBox)

Demo

Be careful at University

A lot of trivial matters are considered punishable

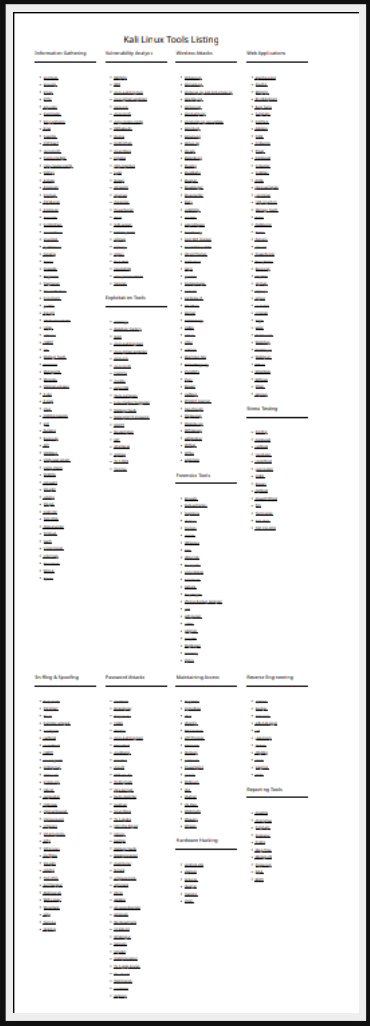
- Sending malware over the network (even to controlled computers)
- Port Scans **!!!**
- Running metasploit on the network **!!!**
- Using UNSW ICT resources to attack of compromis any other system **!!!**

What you should have ready for next week

- VM software installed
- A Linux VM
  - We strongly recommend Ubuntu Budgie
- An attempt at a CTF challenge

Why not Kali?

Who knows what these tools do?


Kali Linux Tools Listing

Information Gathering

Vulnerability Analysis

Wireless Attacks

Web Applications

Exploitation Tools

Stress Testing

Forensics Tools

Sniffing & Spoofing

Password Attacks

Maintaining Access

Reverse Engineering

Hardware Hacking

Reporting Tools

UNSW ICT Acceptable Use Policy

https://my.unsw.edu.au/student/resources/ComputingCommunicationRule.html

You are bound by this as a student.

It has the lowest penalties, but is the one under which you are most likely to be caught.

It is also the most restrictive – some things are legal but not considered acceptable.

Issues faced by previous students and staff include:

- Putting a Kali Linux computer on the UNSW (wired or wireless) network
- Intentionally putting live malware or exploit code over the UNSW network
- Running Metasploit servers on the UNSW network.
- Intentionally bypassing security restrictions without prior authorisation.

In some cases these were unintentional and in some cases these were intentional.

- There have been serious penalties associated with these issues.

If in doubt, ask.

- There are some knowledgeable people in ICTS
- You can get authorisation for some things

Q/A