GETTING STARTED WITH CYBERSECURITY AND CTFS

Joel Kores

WHAT IS CYBERSECURITY?

- IS THE PROTECTION OF COMPUTER SYSTEMS AND NETWORKS FROM INFORMATION DISCLOSURE, THEFT OF, OR DAMAGE TO THEIR HARDWARE, SOFTWARE, OR ELECTRONIC DATA, AS WELL AS FROM THE DISRUPTION OR MISDIRECTION OF THE SERVICES THEY PROVIDE.

Wikipedia

WHAT IS HACKING?

Is to break into computers and computer networks

TYPES OF HACKERS

White Hat

Red Hat

Grey Hat

Black Hat

CYBER SECURITY TEAMS

RED TEAM
Work on the offensive side of cybersecurity

BLUE TEAM
They are the defenders and work on the defensive side.

PURPLE TEAM
With experience in both blue and red team operations.

FOUNDATIONAL SKILLS NEEDED

- Linux Fundamentals
- Windows Fundamentals
- Networking Fundamentals
- Coding/Scripting Fundamentals

CAREERS IN CYBERSECURITY

- Penetration Tester
- Bug Bounty Hunter
- Vulnerability Researcher
- DevSecOps
- Security Software Developer
- Source Code Auditor
- Information Security Analyst
- SOC Analyst
- Cyber Security Specialist
- Information Assurance Engineer
- Security Consultant
- Forensics Expert
- Malware and Threat Hunter

GAINING SKILLS

- Online Courses and Certifications
- YouTube
- Articles
- CTFs

CTFS

Stands for Capture The Flag

They are Gamified hacking competitions whereby the competitors are given various challenges in which they are supposed to find flags and earn them points. Gives the participants experience in security and real world problems

FLAGS

- Flag == <n> points
- Often a hash OR some formatted string.

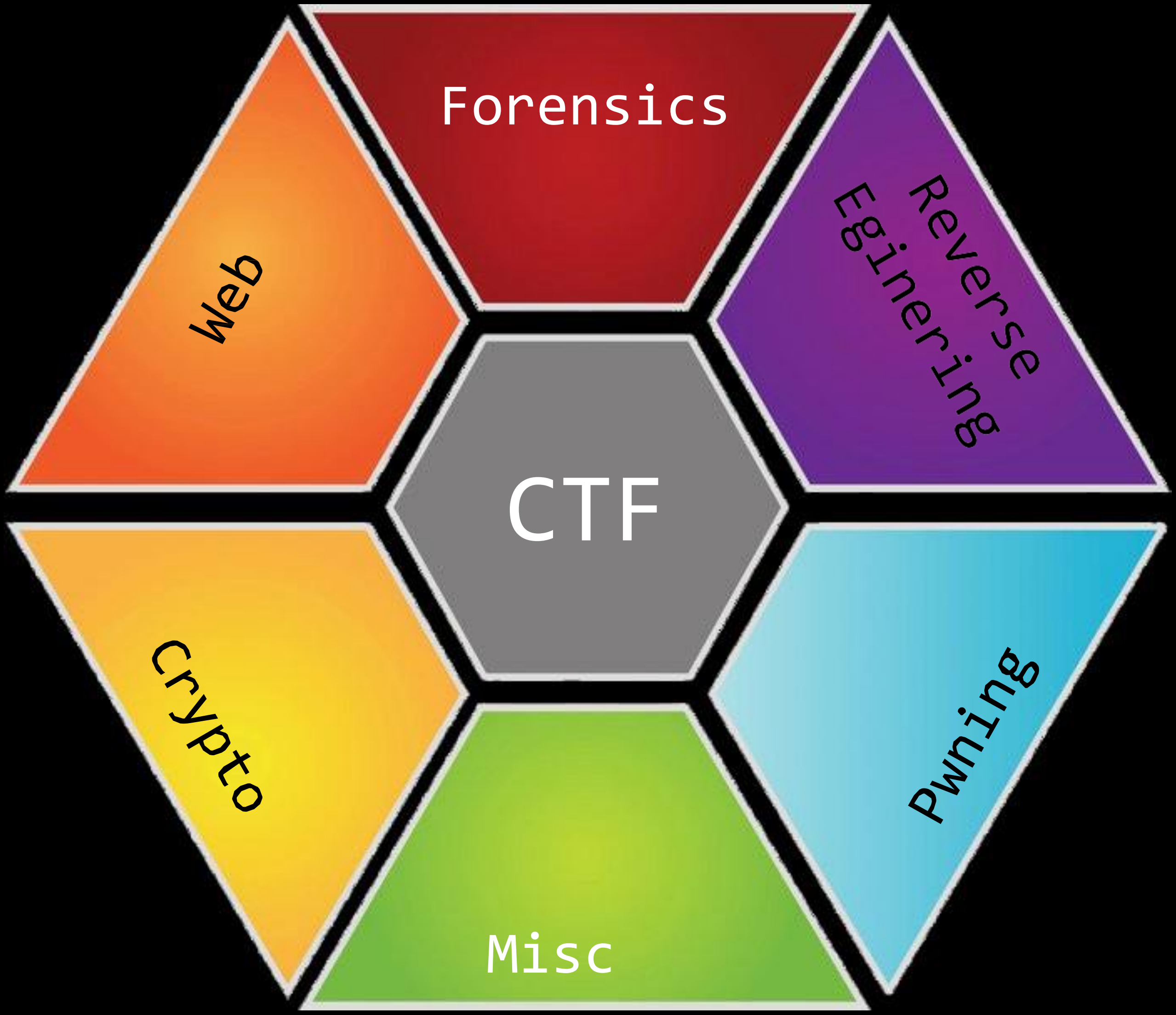
GAME MODES

- Jeopardy
- Boot2Root
- Attack / Defense

JEOPARDY STYLE

- Solve challenges to collect flags
  - Different disciplines
  - Various complexity levels
- Often: First solver receives a bonus
- Most popular version

SOME OF THE DISCIPLINES IN JEOPARDY



- Web
  - (In)Security of web applications
    - SQL injection
    - directory traversal
    - exploiting logical flaws
    - ...
- Forensics
    - Needle in a haystack
    - „Broken“ data / files
    - Image recovery

- Reverse Engineering
  - Understanding algorithms
  - Defeating anti--analysis mechanisms
  - „crackmes“
- Crypto
  - Implementation flaws
  - Efficient attacks

- Pwning
  - Exploitation of services
  - Remote Code Execution (RCE)
  -

- Misc
  - Guessing
  - Recognizing network protocols, file formats, ...

BOOT2ROOT

- Given a vulnerable virtual machine
- Solve and get the root flag
- „equivalent to getting system admin privileges.
    - Hack The Box

b00t2root

ATTACK / DEFENSE

- Every participating team receives the same server image / virtual machine
  - Harden the services in your instance (!= port blocking)
  - Attack vulnerabilities in the other teams‘ services
- Mostly pentesting oriented

King of the hill - THM

WHY PLAY?

- Experience on how security breach can happen
- Meet nice people & have a good time :)
- Learn from failure
- Opportunity for Research
- Great opportunity to learn
- Extend your horizon
- Fame & Glory
- Helps build critical thinking skills

PLATFORMS

HackTheBOX

TryHackMe

CyberRanges

Ctfroom

PicoCTF

Cybertalents

Pwnable kr

Overthewire

Portswigger

Vulnhub

Offsec labs

CTFTIME

COMMUNITIES

Bsides Nairobi

SheHacks KE

AfricaHackOn

Cybercon KE

THANK YOU

in Joel Kores

@K0r3s