Date: 28th June 2021

Konnexions – IT and Web Development Society

Kalinga Institute of Industrial Technology - Deemed to be University, Bhubaneswar

Role: **Ethical Hacking Trainer**
Type: **Community Learning Initiative (Volunteer)**
Period: 20th August 2020 - 30th April 2021

SUMMARY:

Assisted as the Lead Trainer to a *Training-cum-Certification* Ethical Hacking course for undergraduate students looking to enter the Cybersecurity industry and become a skilled security specialist! The course covered prerequisite topics introducing the students, to information security, Linux environment, and pentesting. Motivated beginners and provisioned them with the information required to start a career in Cybersecurity. Adapted to the pandemic and devised a unique way to cater to the students' needs outside the classroom sessions, guided them throughout for 6 months and concluded the course with a 100% practical hands-on evaluation and a theoretical mini-exam, customised to meet the standard industry requirements.

TARGET AUDIENCE:

Undergraduate app and web developers, programmers, students looking to enter the field of Cybersecurity.
Organized an orientation webinar for the same, gave a presentation with engaging visuals.

SESSION DETAILS:

Total – 9 days (Class) + 2 days (Evaluation)
Duration – *90-120 min* LIVE Weekend sessions
Extra – Doubts sessions (On-demand)

PRE-REQUISITES

Basic computer science and programming knowledge.

COURSE CONTENTS:

Day-1: Basics of LINUX & Networking
Introduction, Setup the Lab, Linux commands, staying anonymous

Day-2: Reconnaissance / Footprinting
Information Gathering, Google Dorks, Network Scanning, Shodan

Day-2(II): Scanning & Enumeration
IP, Port, OS and vulnerability scanning using NMAP, LinPEAS

Day-3: System Hacking
Developing malicious Windows and Android payloads in Metasploit

Day-4: Web Application Pen-testing – I (Metasploitable2)
Basic Web concepts, Burp Suite, SQL Injection, LFI & RFI

Day-5: Web Application Pen-testing – II
Cross Site Scripting (XSS), Arbitrary File Upload, RCE

Day-6: Mid-course Evaluation

Day-7: Wireless Hacking
WiFi password cracking using Wireshark and Aircrack-ng

Day-8: Session-Hijacking / Man-in-the-Middle Attacks
Cookie grabbing using XSS, MITM attacks using arpspoof in Kali

KALINGA INSTITUTE OF INDUSTRIAL TECHNOLOGY

MERIT CERTIFICATE

Date: 18th April 2020

Name
Saket Pandey

University Roll Number
1806413

student of
Information Technology

has successfully completed the training in
ETHICAL HACKING

during Autumn Session 2019-20
from
20th July 2019
to
20th October 2019

Reference No. KIIT/KONNEXIONS/2019-20/Autumn/TC/ 017

IT & Web Dev Society
KONNEXIONS

Shubham Agarwal
Student Coordinator,
IT & Web Development Society,
KIIT Deemed to be University

Dr. Chittaranjan Pradhan
Faculty in charge
IT & Web Development Society,
KIIT Deemed to be University

Sample Official Certificate

Day-9: Cryptology
Different encryption and cryptographic methods.

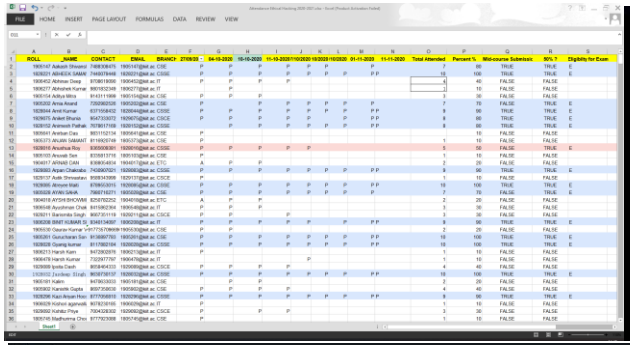
Day-9(II): Brute-Forcing and Fuzzing
Using tools like Hydra and John, Fuzzing on the web

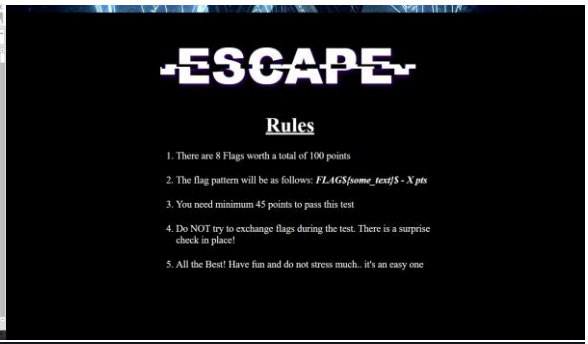
Day-10: CTF Methodology, Solving a CTF Pwnbox (*Rickdiculously Easy - Vulnhub*)
Tools, Methods, Scripts and sources to refer for CTF's and real-world pentesting.

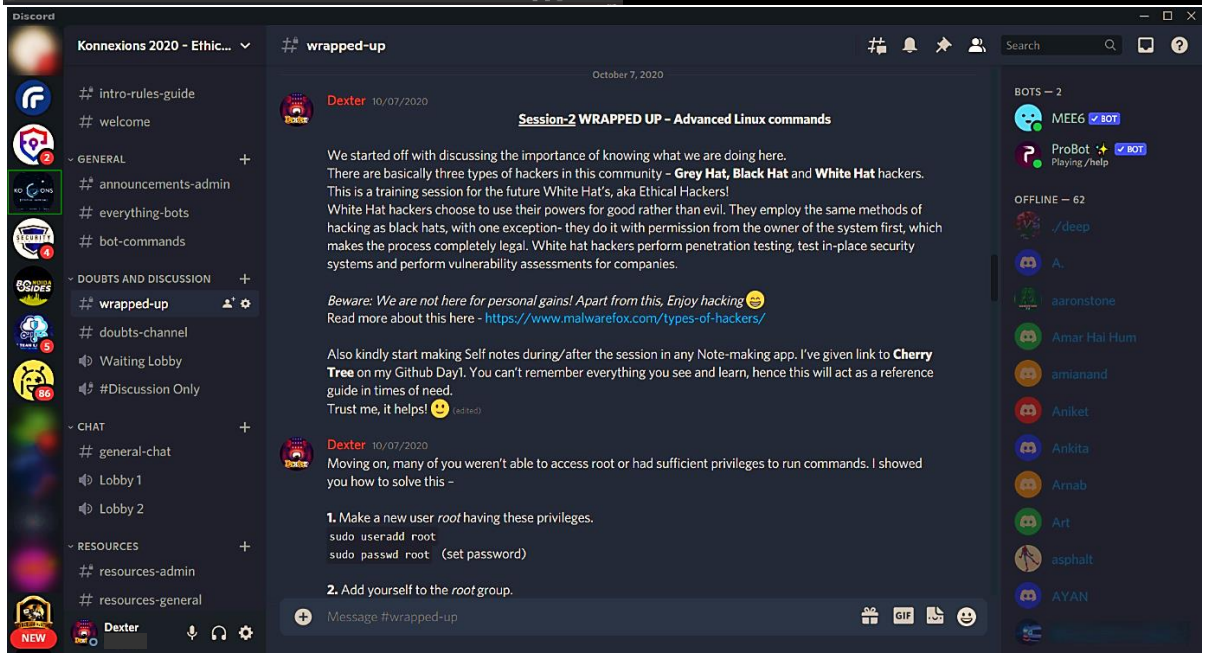
Day-11: Certification Exam (Theory + Practical)

MANAGEMENT METHODOLOGY:

Owing to the pandemic situation, a new virtual method had to be devised to keep the course interesting and interactive, along-with keeping it clutter-free. Sessions were organized only in the weekends over Google Meet, constantly keeping a track record of attendance using a browser extension. Rest of the week consisted of small non-mandatory practical assignments. Facilitated a Discord channel to address student's doubts during the week, and also for the students to know each other, interact, share ideas and solve challenges together. Communicated any and all announcements and invitations through Whatsapp and email. Provided everyone with a "Wrapped Up" document after a session, summarizing that day's topics briefly with all the used tools/commands. If required, gave recordings of certain exploit methods too.







GITHUB LINK – https://github.com/dexter-11/KIIT-Konnexions-2020

ABOUT THE EVALUATION:

Mid-Course (Nov 2020)

Included 6 TryHackMe rooms to complete of which 5 were mandatory to pass.
Topics - Nmap, Metasploit, Google Dorking, Introductory Researching, File Inclusion, Linux Ninja Skills
Students were free to solve the machine without any restrictions on resources.

Final (Jan 2021)

- Created the **CTF** environment in a period of 1.5 months starting December 2020. This was my first box creation which explains the amount of time dedicated. Utilized resources from Github and implementation of vulnerabilities from HackTheBox, referred videos on how to develop the vulnerability in a server and then tested for exploitation. Made sure that no un-intended exploitable paths were present. Graduated seniors provided me with valuable feedback for improvement.
  A walkthrough was made available post-exam for students to practice and reflect on later.
- **Theory Exam** consisted of basics of security and exploitation, and Linux.

PASSING CRITERIA:

This was kept very flexible to support a fair continuous evaluation process. The outline is as follows:

Final CTF (To pass) Min=50m, Max=60m [Total= 5m + 5*10m + 15m + 30m]
Final Theory 30m
Attendance (%/10)m
Mid-course Evaluation 0/-1m
Bonus (Getting Root in CTF 2m + Full Score in Theory 1m)

RESULT:

There were a total of 81 students admitted to the course. ***12 students*** attained **Merit** out of the eligible.
Received Letter of Appreciation from the head of department for my excellent team-management skills and the ability to lead and coordinate with the masses.

POST-TRAINING WORK:

Conducted recruitment of eligible and competent junior trainers to teach in the next session/batch of students. It was a two-level process, Written Test followed by a Personal Interview.

MY THOUGHTS ON THIS EXPERIENCE:

As said, “No warrior left behind!”
You cannot succeed in your field without giving back to the community what you learned. Teaching under Konnexions helped me develop as an individual and as a student. Even I, as a trainer, got exposed to undiscovered perspectives given by students, which helped me polish my knowledge and learn on-the-go. The doubts forced me to look at things differently, and think on how to explain the solution in an understandable manner. This experience tested my patience and organizing skills, and I can proudly say that I stood upto the expectations of this organization. I’ll continue to give back to the community in some form or other and make effective education easily accessible in the coming future.

THANK YOU!