INTERNET APPLICATIONS(CS4400) : MODULE FINAL REPORT

Sudhansh Mehta,TCD 16340820

December 18, 2018

1 InfernoBall Team Self-evaluation

- Team Number: 26
- Team Members
  - Sudhansh Mehta
  - Lal Singh Dhaila
  - Geetanjali Singh
  - Mark Grennan

Evaluation Parameters	Sudhansh Mehta	Lal Singh Dhaila	Geetanjali Singh	Mark Grennan
Effort	High	Medium	Low	Low
Effectiveness	High	High	Medium	Medium

2 Learning Outcomes(What I Learned)

- Design,construct,document,deploy and test scaled distributed system solutions in realistic real-world applications like penetration testing.
- Using on-demand cloud computing platforms like Amazon Web Services(AWS) and Google Cloud Platform for providing Scalable solutions.
- Detailed analysis and comparison of recent advancements in Edge Computing and IoT(Internet of things).
- In depth knowledge and insight into password recovery and hash cracking techniques using tools like Hashcat and John the Ripper.
- Using OpenCL for parallel computing.
- Understanding and extracting major takeaways/points from research papers
  - Identifying recurring themes in the research paper and major ideas mentioned by the authors revolving around those recurring themes.
  - A great focus on Index Terms and extracting the important takeaways from the Abstract of the research paper.
- Writing an effective abstract for an academic research paper.
- A need for effective documentation as is necessary in any software development scenario(helps in being exhaustive especially at a group development stage).

3 Design and Implementation, Methodologies (What I Did)

3.1 Techniques applied for password recovery/hash cracking

- Identifying major Word Lists for cracking hashes from a wide variety of major word lists available.
- Initially attacking the file containing hashes against the Identified word lists(direct attacks).Identifying patterns in cracked passwords : an inherent information embedded in the hashes and the cracked passwords
  - The length of the cracked passwords.
  - The recurring pattern/sequence (letters/digits/special characters/-combination of all) within a cracked password.
  - The recurring pattern/sequences amongst multiple cracked passwords(for both length and recurring sequence of letters/digits/special characters/combination of all).
- Based on the patterns identified as mentioned aforesaid a detailed analysis led to identifying certain masks (mask attacks) or combination attacks appropriate for attacking the uncracked hashes with a faster recovery rate.
- Based on aforementioned analysis the dictionaries were modified as mentioned below
  - The length of the dictionaries was limited at a certain limit or between a certain range.
  - Multiple dictionary combinations were tried for combination attacks after identifying the length and the recurring sequence
  - Each dictionary was thus modified based on the identified pattern(to obtain multiple dictionaries out of one base dictionary) and to Scale the hash recovery process were thus put on multiple instances to run in a parallel fashion with different unique attacks.
  - Finally the different potfiles(cracked hashes) were merged into a single potfile.
- A continuous evaluation and analysis of obtained potfile at various stages throughout the process to identify more precise patterns for recovering hashes.

3.2 Scaling the resources based on Resource Requirement of the task

- During the initial phase of assignments for identifying/ researching the appropriate methodology to be applied for password recovery the brute force techniques were first applied on local machines (containing a MSI GeForce GTX 1050Ti Graphics card) as the cost/credits had to be kept in mind.

- Based on advanced techniques identified as mentioned in Section 3.1 the resources were scaled (based on need)

  - On demand Cloud computing platform Amazon Web Services(through AWS/Rosetta Hub Educate initiative) was employed initially which was sufficient till Assignment 5(InfernoBall assignment).
  - During the InfernoBall assignment a need of stronger GPU's was realized hence a need to offload computation to Google Cloud Platform(another on demand cloud computing platform by Google) which had more powerful GPU's available (NVIDIA Tesla P100 GPU's).

- For the final assignment(InfernoBall) another Scalable factor(personnel factor) was introduced into the system. To optimize the cracking of the Inferno Levels

  - The Identified/earmarked modified word lists (dictionaries) were further divided into the number of people in the group.
  - The Identified/earmarked hash attacks for a particular level were divided into the number of people in the group.
  - The obtained potfile from combining the potfiles of all the members in the group was put to analysis to modify the attacking strategies.
  - All the different kinds of passwords were equally distributed among the members of the group. As it was necessary to crack k of the total passwords in a particular level it was noticed that certain types of hashes were easier to crack than the rest. On identifying the certain type of hashes the focus was to crack the maximum hashes in those hash types.Hence the hashes were distributed and re-distributed based on the aforesaid strategies.

4 Module Evaluation

4.1 Likings

- Hashing as an effective example to practically understand Scalability as a Concept.
- An In-depth coverage of various concepts/ideas involved in developing Scalable Systems.
- Paper Reviews/condensing academic papers to four key points.
- A focus on practically implementing the Scalable solutions supported by theoretical concepts imparted in lectures.
- Interesting Guest lectures to gain an insight into various disciplines thus improving the understanding of Scalability as a concept applied in different domains.

4.2 Dislikings

- Hashing as the sole practical concept to demonstrate Scalability in Systems. Although a perfect example but a curiosity to be exposed to multiple scenarios for implementing Scalable solutions.

5 Latex Link

https://www.overleaf.com/read/sxdzwvyxzbbr