Characterizing Attacker Behavior in a Cybersecurity Penetration Testing Competition - Notes

Cameron Noakes

November 2021

1 Sentence Overview

aim: to assist developers and administrators in providing an idea for an attackers mindset in cyber security penetration testing competitions. Collection of past data from the dataset of events during the 2018 National Collegiate Penetration Testing Competition used identify and exploit vulnerabilities.

2 Abstract - Notes

Acknowledgement of in order to know how an attacker thinks you need to think like an attacker in order to better understand the mindset behind the adversarial attacker.

The group found and exploited seven (7) vulnerabilities, the given approach was then arranged into tactics and techniques within the Mitre Attack Framework.

3 Introduction - Notes

This section helps to explain how thinking like an adversarial attacker when developing and implementing code can lead to more secure systems since the developers are thinking outside the box when it comes to software system security.

Categorising the typical ways in which attackers discover and exploit vulnerabilities can lead to more secure systems when implementing due to developers understanding what features of the software solution could potentially contain unknown vulnerabilities.

Analysis of a 500 million event dataset from six (6) teams from the 2018 National Collegiate Penetration Testing Competition (CPTC'18) allowed offensive and defensive perspectives to be inferred in regards to the Mitre Attack Framework tactics and techniques.

4 The Competition and Dataset

The competition consisted of nine (9) teams in which all would have an identical cyber infrastructure of a fictitious ride sharing organisation titled 'WHEELZ'. The infrastructure was structured of four sub-networks (vdi, corp, prod, and auto).

The dataset was a collection of events captured and indexed by Splunk, a log aggregation platform. Each host in the competition was created with a Splunk agent which periodically captured information from various sources on the host

5 Vulnerabilities

The 500 million event record dataset contains all information on the vulnerabilities with additional metadata to help categorise, filter and sort each event into corresponding orders the observer wishes.

The competition contained a total of 74 known vulnerabilities the attackers could exploit in order to compromise systems, networks and alike to achieve points to rank higher than other teams with each vulnerability ranging in difficulty.

6 Mitre Attack Framework

Brief overview of the Mitre Attack Framework was given and how it is a knowledge base for common industry tactics and techniques in order to offensively compromise systems or software but also a latter option for defensive measures to counteract the offensive processes.

A description of how the Mitre Attack Framework is used for enterprise networks and also mobile communication devices and the main focus being on enterprise networks due to the competition heavily resembling this type of network more than the other. There is a limitation however, about how the researcher did not additionally add other sectors the Mitre Attack Framework is used for such as web application security.

7 Evidence Gathering - Reports

Reports were submitted by the teams at the end of the competition to outline the successfully accomplished attacker the team underwent. These reports can be speculated to be industry standard penetration testing reports which would clearly outline the vulnerabilities present and exploited.

Examples of exploiting a vulnerability were given: ”For instance, an attacker can discover the MongoDB vulnerability by actually connecting to the MongoDB instance from a remote host without providing any credentials (i.e. by exploiting the vulnerability).”

8 Attackers Perspective

The knowledge of the timestamp of the attack in the dataset and possibly the reports, considerably reduces the number of events to read through since it can provide an instance in time from which to work backwards from to identify the attacker's actions, allowing more coverage of the attacker mindset when it comes to exploiting vulnerabilities.

9 Limitations the paper discusses

An explained limitation in the paper is related to how the report (for example from team one (1)) concluded an exploitation by dumping the MongoDB database but there was no record of such activity in the dataset scraped. This created gaps in informational knowledge which in turn creates gaps in the research due to information being missing.

However, the researchers did not leave the reports out which managed to gather lots of duplicate data in comparison to the reports and the datasets but did find small pieces of information relating to the exploitation of vulnerabilities that one of the options may miss but the other picked up.

10 Research Gaps and Questions

A research gap that was not discussed is that due to the vulnerabilities being in ranged severity and difficulty, this could influence the attackers perspective and mindset and alter their actions due to this.

How would they counteract this?
Would they take this into account and if so, how?

11 What problem does this solve?

Developers often focus on developing software and system solutions and security is left for a further away deadline, providing attackers a head start when exploiting vulnerabilities they have not dedicated resources for to fix yet.

By educating developers on how to write secure software this can reduce the risk and number of attacks on company assets since the solutions are more secure and also do not need to dedicate resources in the future to outlining and fixing vulnerabilities that were already remediated upon development.

12 How do they solve it?

By analyzing some 500 million records within a dataset from a penetration testing competition outlined key information regarding the mindset behind attackers and how defensive operational teams can mitigate vulnerabilities to a better standard.

13 How do they assess it?

Assessing the proposed solution would be done through the concept of if the defensive teams, developers and alike are more educated on potential attacks for the software they create or the systems they protect.

Real world competition data was evaluated and analysed which conclusively ascertained the methodology behind an adversarial attackers perspective and mindset, allowing for defensive teams to adopt the same mindset to secure systems superiorly.

14 Conclusion - Notes

Conclusive statements are that the 500 million dataset records aided in the exploration of concepts behind the attackers perspective, outlining the mindset so other industry technology professionals can adopt the same mindset when it comes to their duties.

The paper shows that characterizing attackers' campaigns as a chronological, ordered sequence of Mitre Attack tactics and techniques is feasible and such a characterization can inform the attacker mindset to developers and administrators in their pursuit of secure software systems.