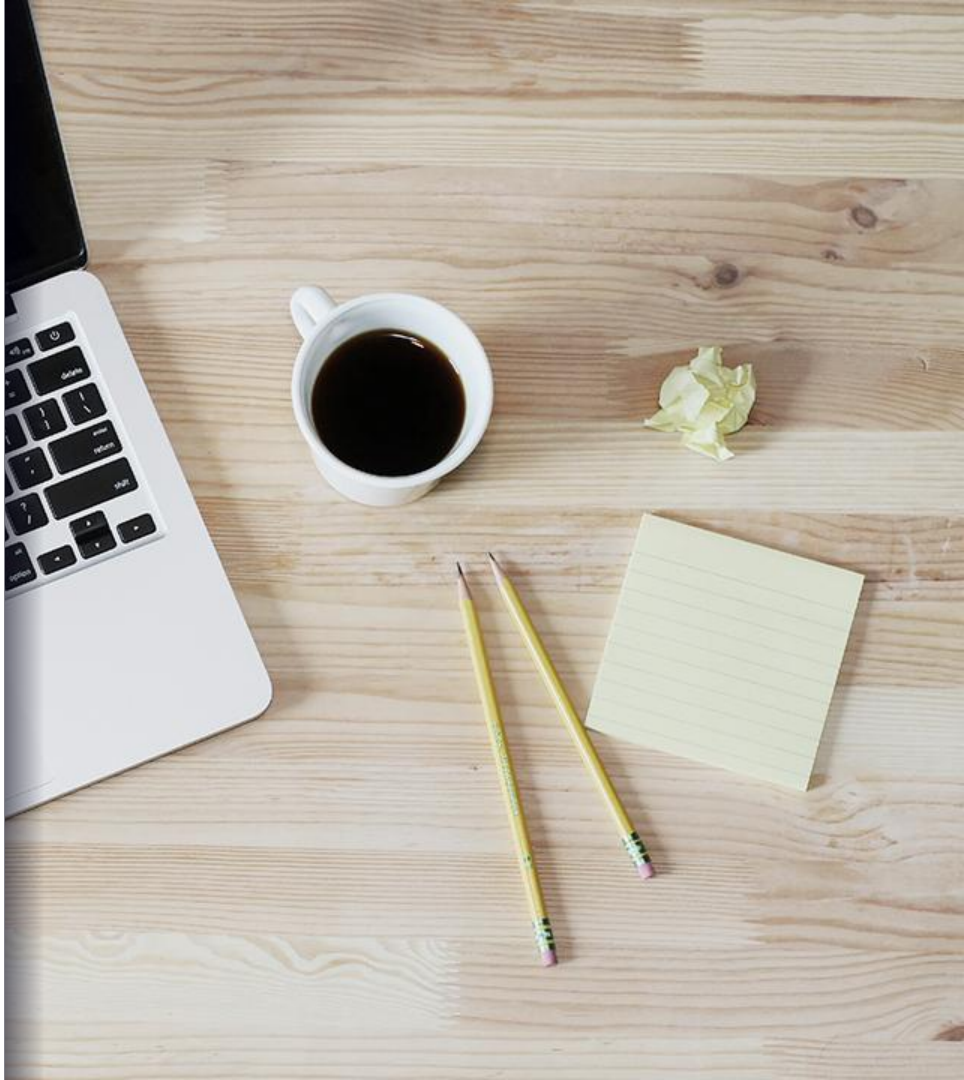
THE ATTACK OF HOPSCOTCH



WHY DID WE CHOOSE THIS TOPIC?

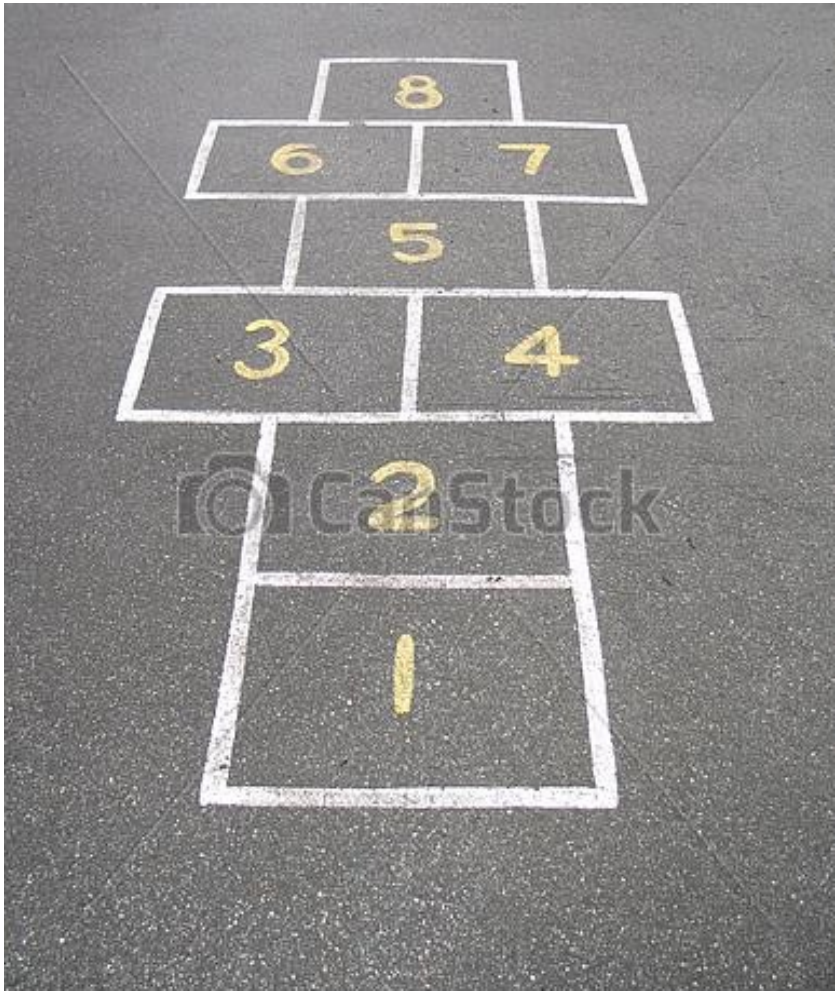
Hopscotch was found to be present in the top 10 vulnerabilities in the world. This vulnerability

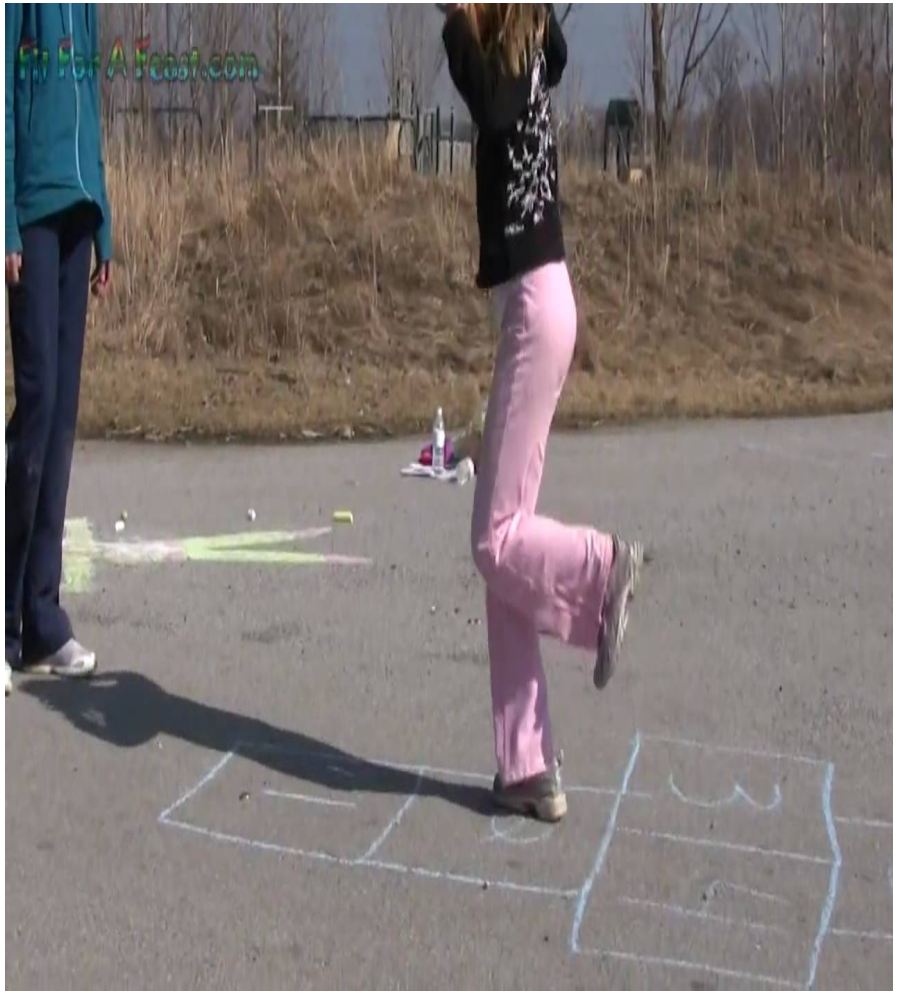
is based on similar lines of the game of hopscotch.

Before we begin with the explanation of this vulnerability let us see what is the game of hopscotch ?

THE GAME OF HOPSCOTCH

Hopscotch *is a children's* ***game*** *that can be played with several players or alone.* ***Hopscotch*** *is a popular playground* ***game*** *in which players toss a small object into numbered triangles or a pattern of rectangles outlined on the ground and then hop or jump through the spaces to retrieve the object.*


8
6
7
5
3
4
2
1



HOPSCOTCH:THE VULNERABILITY

Rather than taking advantage of buffer overflow and gaining complete access to a database in the first stage, cybercriminals often play a game of Hopscotch: finding a weakness within the infrastructure that can be used as leverage for more serious attacks until they reach the back-end database system.

FOR EXAMPLE :

A hacker may worm their way through your accounts department before hitting the credit card processing arena. Unless every department has the same standard of control, creating separate administrator accounts and segregating systems can help mitigate the risk.

THE ATTACK OF HOPSCOTCH IN HEARTLAND PAYMENT SYSTEMS

In the Heartland Payment Systems breach, attackers first gained access to the accounting group, which led to access to the credit card processing systems.

THE STEPS FOLLOWED IN THE ATTACK:

- *>> The initial breach was to a nonfinancial system.*
- *The transaction network was segregated.*
- *>> Attackers used xp_cmdshell to gain a foothold, install*
- *malware and begin scanning the environment.*
- *>> The compromised system had VPN access into the*
- *transaction network and connected while the attackers*
- *were remotely monitoring.*
- *>> The attackers used that connection to bridge networks*
- *and install malware. The malware was sophisticated and*
- *designed by a former financial programmer.*
- *>> 130 million credit card numbers were exposed.*
- *>>The incident resulted in a $60 million settlement with Visa.*

POSSIBLE WAYS OF AVOIDING THE ATTACK:

- *It is highly recommended that networks , servers and applications — including databases — have separate admin accounts,passwords and personnel.*
- *At small and midsize firms there typically isn't a team of database administrators, but rather one person who performs both database and server administration duties. Still, it is highly recommended to use segregation of systems*
- *It's important to disable features that would allow easy transition from an application to a server, or viceversa.*
- *For example, external stored procedure allow an attacker to execute arbitrary database commands simply by gaining access to the platform, or to run system commands solely by getting access to the database. Trust boundaries that give legitimate users easy means to hop among services make it easier for attackers to do the same.*

THANK YOU