# Article information:

Detecting stealthy, distributed SSH brute-forcing
<https://dl.acm.org/doi/epdf/10.1145/2508859.2516719>

# Article summary:

1. Researchers have developed a detector to identify stealthy, distributed SSH brute-forcing attacks that would be missed by point-wise host-based detectors.

2. The detector was evaluated on 8 years of SSH login records collected at the Lawrence Berkeley National Laboratory and found multiple large-scale coordinated attacks from botnets, some lasting up to 1.5 months.

3. The prevalence of SSH brute-force attacks has been studied in previous research, with recurring activity targeting a wide range of IP address space and instances of slow and distributed attacks designed to evade detection.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article discusses a new approach to detecting stealthy, distributed SSH brute-forcing attacks. The authors develop and evaluate their detector on eight years of SSH login records collected at the Lawrence Berkeley National Laboratory. They measure and quantify the duration, intensity, and behavior of the detected attacks and find multiple large-scale coordinated attacks from botnets.

The article provides a comprehensive review of related work in three domains: coordinated attack detection, SSH brute-force attack detection, and studies of the prevalence of SSH brute-forcing activity. However, the article does not provide enough evidence to support its claims that its approach is superior to existing methods. The authors claim that all the attacks they detect would have been completely missed by a point-wise host-based detector. Still, they do not provide any evidence to support this claim.

The article also lacks discussion on potential biases or limitations in their approach. For example, it is unclear how their detector would perform against more sophisticated attackers who use techniques such as password spraying or credential stuffing instead of brute-forcing.

Furthermore, while the authors discuss the prevalence of SSH brute-force attacks in previous studies, they do not explore why these attacks are so prevalent or what can be done to prevent them. Additionally, there is no discussion on potential risks associated with detecting these attacks or how false positives could impact legitimate users' access.

Overall, while the article provides valuable insights into detecting stealthy SSH brute-forcing attacks, it lacks sufficient evidence to support its claims and does not address potential biases or limitations in its approach adequately.

# Topics for further research:

* Strategies to prevent SSH brute-force attacks
* Password spraying and credential stuffing techniques in cyber attacks
* Limitations of point-wise host-based detectors in detecting SSH attacks
* Risks associated with detecting SSH brute-force attacks
* False positives in SSH attack detection and their impact on legitimate users
* Best practices for securing SSH access and preventing attacks

# Report location:

<https://www.fullpicture.app/item/43e9f9d0b917183c04b9eb888ca0238c>