# Article information:

Profiling Attacker Behavior Following SSH Compromises | IEEE Conference Publication | IEEE Xplore
<https://ieeexplore.ieee.org/document/4272962>

# Article summary:

1. The article presents the results of an experiment aimed at building a profile of attacker behavior following a remote compromise.

2. Four Linux honeypot computers running SSH with easily guessable passwords were utilized for the experiment.

3. Specific actions taken by the attacker and the order in which they occurred were analyzed to build a profile of attacker behavior, including checking configuration, changing password, downloading files, installing/running rogue code, and changing system configuration.

# 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 titled "Profiling Attacker Behavior Following SSH Compromises" presents the results of an experiment aimed at building a profile of attacker behavior following a remote compromise. The article provides valuable insights into the most commonly attempted usernames and passwords, the average number of attempted logins per day, and the ratio of failed to successful attempts. However, there are several potential biases and missing points of consideration that need to be addressed.

One potential bias in the article is that it only focuses on Linux honeypot computers running SSH with easily guessable passwords. This limits the scope of the study and may not accurately reflect real-world scenarios where attackers use more sophisticated methods to gain access to systems. Additionally, the article does not provide any information about how long the honeypots were active or how many attacks were recorded during that time period.

Another potential bias is that the article only looks at specific actions taken by attackers following a compromise, such as checking configuration, changing passwords, downloading files, installing/running rogue code, and changing system configurations. This narrow focus may overlook other important actions taken by attackers, such as exfiltrating data or creating backdoors for future access.

The article also lacks evidence for some of its claims. For example, it states that attackers typically change passwords after gaining access to a system but does not provide any data to support this claim. Similarly, it claims that attackers often download files but does not provide any information about what types of files are downloaded or why.

There are also missing points of consideration in the article. For example, it does not address how organizations can use this information to improve their security posture or prevent future attacks. It also does not consider how attackers might adapt their behavior in response to increased awareness of these tactics.

Overall, while the article provides valuable insights into attacker behavior following SSH compromises, there are several potential biases and missing points of consideration that need to be addressed. Organizations should take this information into account when developing their security strategies but should also consider other factors that may impact their risk profile.

# Topics for further research:

* Strategies for preventing SSH compromises beyond easily guessable passwords
* Real-world scenarios of SSH compromise and attacker behavior
* Actions taken by attackers beyond those mentioned in the article following a compromise
* Evidence supporting claims made in the article about attacker behavior
* Using information on attacker behavior to improve organizational security posture
* Adapting security strategies in response to increased awareness of attacker tactics

# Report location:

<https://www.fullpicture.app/item/e493563afd9cf06666e9d68752894aa2>