Emergency Actions After Hacking

# Abstract

This paper describes the reactive measures that should be taken after hacking. As the world is moving towards wireless digital technology and everything is directly or indirectly internet connected. Hacker always trying to exploit vulnerability in the system. If Attackers attack the system one time, it is most likely that this attack will happen again with high intensity. Hence It is highly recommended that take threats seriously and understand the risk and potential loss that could occur. Because the nature and purpose of every attack are different, there is no single prevention and prescription. But we can follow certain steps as a general guideline after the attack like, identify the damage and record the details, communicate the incident to the larger group, try to limit the further damage, see the legal aspect if the breach could be reported to the law enforcement agency. In this paper we will discuss about these aspects in details.

# Introduction

To begin with let’s first understand the word hacking. A commonly used hacking definition is the act of compromising digital devices and networks through unauthorized access to an account or computer system. Hacking is not always a malicious act, but it is most associated with illegal activity and data theft by cyber criminals. The main key drivers that lead to bad actor hacking systems a) Financial gain through the theft of credit card details or by defrauding financial details b) Corporate espionage c) to gain notoriety or respect for their hacking talent c) State sponsored hacking that aims to steal the business information and national intelligence. In addition to that there are politically motivated hackers , who aim to raise public attention by leaking sensitive information such as WikiLeaks.

A few most common types of hackers are Black hat hackers “bad guys”, they go out of their way to discover vulnerabilities in the systems and software to exploit them for financial gain, or for malicious purpose, such as gain reputation, carry out espionage, stealing the data and sell it to black market. White hack hackers can be seen as “good guys” who attempt to prevent the success of Black hat hacker through proactive hacking, they test the levels of system security, this helps to expose vulnerabilities in the system before black hat hacker can identify and exploit them. Grey hat hackers sit somewhere between good and the black guys. Unlike black hat hackers, they attempt to violate standards and principal but without intending to do harm or gain financially.

In this paper we will talk about the attack done by Black Hat hackers. It is also necessary that proper contingency measure should be in place to secure the system. Many a times organization or victims do not know about the breach, not follow proper emergency action plan, hence this could lead to sever damage in CIA traid (Confidentiality, Integrity and Availability) security models and it produces critical financial or reputation loss. Therefore, we will discuss about attack detection and emergency action after attack in the subsequent paper. Listed below few important emergency actions:

* Estimate the damage (Survey phase)
* Isolate the compromised areas
* Limit the attack from spreading or progressing
* Record the details.
* Attempt recovery and continuity of operations
* Report the attack (Preliminary reports)
* Ensure compliance with legal requirements like informing law enforcement
* Ensure business ethics are maintained. Like informing the customers/clients

**How to Detect Attack**

Emergency response to attack starts with the detection of the attack. Detecting at the attack at the earliest is paramount to mounting an effective response to it. An appropriate response is decided usually based on the type of attack and the stage at which it is detected. There are numerous forms of security automation tools that can help us to detect security attack and take preventive action accordingly. Most common tool is antivirus software, most antivirus detect malware, spyware, ransomware and malicious mail attachment. Other key threat detection strategies may include.

* Monitoring threat detection logs: Logs are generated by network devices, software applications, operating systems, internet of things devices and many other system hardware.

Each device or system generate perform numerous tasks hence generate large numbers of events, for example, security related events are Authentication success event, Authentication failure event, Access control success event, Access control failure event, connection request event, connection failure event, connection success event, Security alarms event etc. Most of the IT systems and Organization employed advanced logging system capabilities, which help them to detect suspicious and abnormal activities. By proper maintaining and reviewing logs. Cyber security expert can conduct detail investigations and monitoring of these logs to detect ongoing or forthcoming attacks. organization also automate these log monitoring task to generate alert based on suspicious or abnormal activities.

* Intrusion Detection System: Network security application or device that monitor and identifies malicious or suspicious activity then report back its result to an administrator system. IDS allow system administrator to configure various alerts and alarms levels associated with it. For example, IDS can be configured to notify them directly via email or call. IDS can also configure to notify external security service of “break in”.

IDs can also perform a variety of functions such as:

a) Monitoring user system activity

b) Auditing system configuration for vulnerabilities and misconfiguration

c) Correcting system configuration errors

d) Recognizing abnormal activity through statical analysis

e) Managing audit trails and highlighting user violation of policy or abnormal activity.

* User and Entity Behaviour Analytics: This security process involves analyses of normal conduct of user behaviour; in turn they detect any anomalous behaviour or deviation from the normal patterns. For example, if a particular user regularly downloads less than 100 MB of files every day but suddenly download tera bytes of files, the system would be able to detect this anomaly and alert them immediately. Behaviour analytics use machine learning algorithms and statistical analyses to identify the abnormal pattern, it can also provide detailed report, flow, logs, packet information of the anomaly behaviour which could result in potential threat. Behaviour analytic track the user and entities in the system instead of just security events to get the insight of suspicious behaviour.
* Honeypot is a one of the cyber security mechanisms that create virtual trap to lure attackers. An intentionally compromised computer system allows attacker to exploit vulnerabilities, so that security team understand attack behaviour and investigate cyber security breaches to collect intel on how cybercriminals operate. There are three types of honeypot deployment that permit threat actors to perform different level of malicious activity.
  + Pure honeypots - complete production system that monitor attacks through bug taps on the link that connect honeypot to the network
  + Low interaction honeypots – imitate service and system that frequently attract criminal attention. They offer a method for collecting data from bind attacks such as botnet and worm’s malware.
  + High interaction honeypots – complex setup that behave like real production infrastructure. They don’t restrict the level of activity of cybercriminal, provide extensive cyber security insight.
* Honeypots/honey farms can be added
* We can illustrate which forms of attacks are detected using which methods.

**Here is the list of few types of Attacks and their detection methods.**

|  |  |  |
| --- | --- | --- |
| **Type of Attack** | **Description** | **Detection** |
| Malware | Software Program designed to damage or do unwanted actions in a computer. Common examples include viruses, worms, Trojan horses, spyware, and ransomware | Annoying pop-up massage on the computer system, system become sluggish at in appropriate time, some files are missing or deleted without the knowledge. Use good antivirus software to detect the malware or virus program. |
| Phishing | Attack sent via mail and ask a user to click on link and enter their personal data. They include link that direct the user to a dummy site, that will steals a user’s information | Look for email address and sender name and make sure it comes from legit user, Check the domain name and URL of the website it should not point to suspicious link. Message do not create sense of urgency, not poorly, containing grammar mistakes. |
| Password Attack | Involves a third party trying to gain access to potential victim by solving a user’s password | High number of authentication attempts, especially failed attempt due to incorrect password within a short period of time. |
| Denial of Service Attack | Attackers send high volume of data traffic through the network becomes overloaded and can no longer function | Monitor for significant increase in TCP-SYN (initial packet to establish a connection), Monitor DNS activity in case of number of DNS request packet will be considerably higher than the number of DNS response packet should be alerted,  Monitor overall throughput and count ICMP packet provide early signs of warnings. |
| Man in the Middle | Information is obtained from the end user and the entity user is communicating with by impersonating the endpoints in an online information exchange (i.e. connection from smartphone to website) | Checking for proper page authentication and implementing some sort of tamper detection are typically the key methods to detect possible attack, but these procedures might require extra forensic analysis after the fact. |
| Drive by downloads | A program is downloaded to a user’s system just by visiting the site. It does not require any type of action by the user to download. | Sometimes it is difficult to detect this attack easily, but proper monitoring of log , flow data and network packets cyber security expert can find out that system is compromised by drive by download attack. |

Now, after detecting the security attack we are in the position to act on it, sometimes it is not possible to prevent the attack completely, one can minimize the damage of the attack or reduce the loss. There are some general courses of actions we take after the attack happened. The purpose of these action is to not repeat the same or similar kind of attack in future.

**Emergency Action After the Attack.**

**Here write detail explanation of each steps**

# REFERENCES (Ensure that all references are fully complete and accurate as per the example. You may check online for more examples)

<https://www.american.edu/kogod/research/cybergov/upload/what-to-do.pdf>

<https://cybersecurityguide.org/resources/cyber-incident-guide/>

<https://www.choosi.com.au/choosi/media/documents/document-what-to-do-if-you-have-been-hacked.pdf>

<https://www.pcmag.com/how-to/what-to-do-when-youve-been-hacked>

<https://www.jigsawacademy.com/what-to-do-if-you-are-hacked/>

<https://socialmediaexplorer.com/content-sections/tools-and-tips/how-to-secure-your-social-accounts-from-hackers/>

<https://www.swisscom.ch/en/business/enterprise/themen/security/data-breach-erste-hilfe-beim-hacker-angriff.html>

<https://teckpath.com/emergency-actions-after-a-hacking-incidence/>

<https://www.uscybersecurity.net/emergency-actions-after-hacking/>

<https://www.hostreview.com/blog/200421-8-emergency-actions-you-should-take-after-hacking>

<https://www.wired.com/2013/03/what-to-do-after-youve-been-hacked/>

<https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/>

<https://www.imperva.com/learn/application-security/honeypot-honeynet/>