A Hacker’s Perspective Risk Assessment Report

In the PC realm, some decent people build systems that assist us with communicating, working with others, and getting data. But there remain individuals who utilize their PCs to illegally hack into people’s systems and cause havoc. As an individual who utilizes a variety of network systems, my goal is to hack into your system and expose all weaknesses and vulnerabilities to help prevent exploitation. The hacker should be taken seriously. A variety of circumstances should be considered. Companies that are experiencing a growth spurt are often a perfect target. Logistix recently was shown in a Fortune publication as an all-American influential achievement story illuminating the development of their small business, its origins, and embracing their accomplishments. The organization currently employs around, 3200 representatives. The organization has been projected to have a constant increase, which is forecasted to keep momentum with S&P ratings for the following six years.

The company is a distribution organization that handles thousands of consumer accounts throughout North America. Logistix went unrestricted and is being exchanged freely on the New York Stock Exchange (NYSE). As the growth potential of the company increases, be aware that this is the picture-perfect opening to attempt network exploitation. Therefore, the Information Technology and Protection departments are challenged to deal with the accelerated development of the company, monitor the vulnerabilities, and weaknesses created by the growth to prevent the network from being exploited. Based on my findings, a risk assessment is recommended for the business.

After researching the Logistix system looking for clues that would help me identify a weakness or a vulnerability that I could exploit. The FTP server became the opportunity of choice. The FTP server will sequentially allow entrance to the organization's network. No event can be completely exploited until the risk assessment is conducted. This vulnerability analysis will assist me in determining the danger against the trophy.

Risks

There are numerous risks associated with any organization. By conducting this risk assessment, four key threats will become evident. The initial threat is to remain undetected. Hackers share the same mindset not to be detected. The consequence is that the Information Technology and Protection division will identify the infringement. Note: even with manipulated qualifications, a security breach can be identified. The hacker’s actions will not be regarded as typical traffic from inside the system but as an abnormality. Access and discovery are required on the main pass within Logistix' s network before exploitation can occur. If the company can identify and trace a danger's existence early on, they will be capable of discovering and insulate the weaknesses before the breach.

Facts: Some devices exist that can detect traffic flow on the system. The Logistixs’ company currently employs an Intrusion Deterrence and Intrusion Discovery System. Intrusion Detection Systems evaluate system interchange for signs that fit well-known cyberattacks. Intrusion Prevention Systems also examine packages and can prevent the package from being distributed based on the type of assaults it identifies.

These systems are intended to identify, examine, and alleviate questionable action on a system (What is the difference between an IDS and an IPS? , n.d.). Logistixs does not depend on customary signatures to identify irregularities. The software also complements conventional virus software and manages network behaviours. (Outlier Security, 2016) The second threat is an operation devised by the police bureaus, presenting a chance to apprehend a hacker. This tactic is known as a honeypot. Honey Pot was created to entice an individual or company to commit an illegal act (The Innocent, 2017).

A Honeypot must be used by well-defined legislation and administration offices to detect and confine perpetrators on all levels. When presented with a system that has the best opportunity for exploitation, one would probably look through the IP addresses and their subsequent entries with NMAP. This can occur when more traditional and old operating policies are identified with NETCAT.

Risk number three is exploitation, indicating the danger of a system infringement by a hacker. There are numerous motives as to why hackers would be targeted, but administrations and organizations are continually examining for instants that they can be exploited. Being hack by way of another intruder can create an unfavourable reputation, lead to information loss, extortion, and practices being banned. The original data collected and purchased to manage an extensive investigation of Logistix. To make certain that the information was gathered, and payment was received, precautions are set in place to assist with the replacement and safeguarding of all valuable information.

Finally, the identified risk factor. The danger of authentication is a risk that usually involves unfavourable consequences. Typically, individuals can be irresponsible by posting private data on social media. This can lead to others examining and discovering the identity of the character in question. The result could be a prison, penalties, extortion, even intimidation into other treacherous actions.

Exploitation & Likelihood

Every threat can have a distinct opponent or several in a combination that is reliant on risk. The first threat is the Information Technology and Defense teams at Logistix. Their job descriptions are to make sure the system and safety measures are operating and to safeguard and maintain the network. Is it possible that exposure and being apprehended can materialize? There is a great probability that when discovery and development occur on the Logistix network, the activity may be exposed. According to Security intelligence, the assessment of the risk player is contingent on several principles, including:

- The dexterity level of the invader;
- The purpose of the player;
- Whether or not the assailant holds the essential information and access
- The competences of the adversary you are engaging, which include economic capitals.

There are various techniques through which an invader can uncover a weakness, such as exploration, testing, and data discovery The strange movement has a high possibility of being uncovered by the Intrusion Protection System and Intrusion Detection System application that is installed on the Logistix network. Yet, the ability to conceal, behave stealthily, and the

manipulation of liabilities will be essential in parallel with the utilization of defence qualifications.

Local, state, and federal who enforce the rule of law, will be identified as the second risk. Bureaus that enforce regulation is continually exploring ideas and practices apprehend a lawbreaker (hacker) in the act of trying to breach a network. The use of honey pots is frequently utilized during various procedures to help catch offenders (TheInnocent, 2017). Centralized groups have been recognized for capturing system criminals utilizing the internet in conjunction with honeypots. Every So Often, bogus sites are constructed, and the goal is to advertise despicable events. Examples are illegal medications, selling firearms, and child pornography. These sites are designed to attract individuals that find the dark web enticing. A hacker knows that data and financial interchange is deemed dangerous. The hacker also understands that the realm of hacking is about obscurity to retrieve information without being detected. These actions are considered an adventure from some or a way of life.

The third risk is the hacker. Now, depending on the skill set of the threat. The hacker, once access to the system has been gained, can be cruel. There is no justification that hackers have a code of ethics hackers do not trust each other. Individuals will take advantage of a situation that they can control and manipulate. If you research the world of infringement and information manipulation you may determine there is no difference. Every so often a group of hackers targets one hacker to exploit then combine assets to and break into an unidentified network. Hackers, today, are employed by businesses to hack into their system and expose all vulnerabilities, weaknesses, and exploitation.

The probability of being utilized by a hacker should always be fear. To help alleviate this, confidentiality is essential. Yet, police agencies, Hackers, Defense, Public Broadcasting Locations, Governments, and Third-Party Players can utilize your identification to target you. The end-result of exploitation can be prison or extortion (Fox-Brewster, 2017).

The Course of Action

How do we alleviate the threat with a suitable course of action to avoid being exposed by the Logistix staff, the police, or another intruder? According to Security intelligence, the lifecycle managing of markers is a vital component throughout event response planning. The lifecycle sway rulings and measures against invaders. It is an endless method of signs of conciliation to ensure the data you utilize is legitimate and beneficial. Readily available are two substantial types of action: reactive and effective (Van Impe, 2017).

Here are several essential procedures that should be undertaken.

1. System Operations should have no remnants for exposure, discovery, and exploitation.
2. The utilization of defence exploitation on the system, backdoors and emergency procedures.
3. The required use of a Virtual Private Network, phoney qualifications, and civic systems are resources. Note: utilizing a Virtual Private Network comes with risks. All VPNs are not identical. While you could be unknown when utilizing a Virtual Private Network, you must understand the risk involved.
4. Avoid the utilization of home internet and utilize a different personal computer when doing the task.

Summary

According to Security intelligence, most contemporary Information Technology defence units utilize threat managing to discover an equilibrium among recognizing openings and reducing prospective losses. Risk managing is more than just a skill; it is the procedure of determining, computing, and highlighting the threats businesses cope with (Van Impe, 2017). Numerous results can arise from the identified risks in the event they are utilized by these dangers. Detecting the initial infringement and acting appropriately will allow for information gathered to be presented to the local policing agency. This event could start an inquiry that might lead to the intruder being identified. Also, a hacker, could access system information and turn a profit.

Logistixs', network, and their system exist at the centre of a changeover. The objective corresponds with the assessment of Logistix being in a picture-perfect situation for the system to be accessed and exploited. The system data collected varies from the workforce's payroll to personal client account data. A data hack that retrieves this type of data can cause a company complexity in the future.