SUMMER INTRENSHIP

TOPIC NAME: Study and analysis of Cyber Security Attacks by using the machine learning with python

ABSTRACT : Cybersecurity is receiving more attention these years because an increasing number of hackings have been reported. Visualization of data can assist in bringing attention to this issue. Log files are used to keep track of all the users that have accessed a server. Charts and graphs can help get a better understanding of the security log files. The IP addresses extracted from log files can be used to track the location of the machines that are trying to connect to the servers. A third-party geo-locating API is available to match IP addresses to identify where the user resides. Google Maps API can mark where the IP addresses are on the map based on the location given. This research focuses on visualizing the unauthorized access attempts on the servers by extracting the user data from the log files that were collected from 3 servers over a 2-month period.

Keywords:

1) Most targeted Destination IP Address

2) Most Logical Ports attacked

3) Most Frequently/common type of Attack

4) Different time of the day , (odd , hours, day or night)

5) Find the Pattern

Types of attacks:

Exploits : An exploit is **a piece of software, data or sequence of commands that takes advantage of a vulnerability to cause unintended behavior or to gain unauthorized access to sensitive data**

Generic : A "generic attack" against a cryptographical primitive is **one that can be run independently of the details of how that cryptographical primitive is implemented**

Reconnaissance : econnaissance is **the practice of covertly discovering and collecting information about a system**. This method is often used in ethical hacking or penetration testing.

Worms : A worm is **a type of malicious software (malware) that replicates while moving across computers, leaving copies of itself in the memory of each computer in its path**. The worm can, for example, carry ransomware , viruses or other malware, which then cause damage to the infected systems. These can then, for example, delete files on the PC or encrypt files in the event of a **blackmail attack**.

Dos : Attackers achieve this by sending more traffic than the target can handle, causing it to fail—making it unable to provide service to its normal users. Examples of targets might include email, online banking, websites, or any other service relying on a targeted network or computer.

Fuzzers : Fuzz testing or fuzzing is **an automated software testing method that injects invalid, malformed, or unexpected inputs into a system to reveal software defects and vulnerabilities**. A fuzzing tool injects these inputs into the system and then monitors for exceptions such as crashes or information leakage.

Shellcode: Shellcode is **a set of instructions that executes a command in software to take control of or exploit a compromised machine**. Read up on the malware term and how to mitigate the risk. It is so named because it typically spawns a command shell from which attackers can take control of the affected system.

Backdoors : A backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka root access) on a computer system, network or software application.

Analysis: raditional information security attack analysis focuses on computer intrusions and malware events in which an attacker gains access or causes damage to a system (or network) through the use of technical capabilities to exploit a vulnerability.

Cybersecurity is receiving more attention these

years because an increasing number of hackings have