Increased Cyber Attacks in Post Pandemic Era-An Analysis and Effective Solutions

Introduction

2020 was an year of turnarounds for entire humankind as well as for the world of internet. The very little things which we never thought will automate has now become completely automated. And as a matter of fact, the relevance of cyber security measures has also now a topic of discussion. While discussing about cyber security, security breaches should also be considered. Covid-19 has paved the way for vast digitalization which we thought will occur only after several years from now. As a result, data transferring through online platforms has increased multiple times. But did we ever thought how securely our data being transmitted or sent to the other person safely without any leakage of information? The answer lies in cyber security. As the automation of services increased the number of cyber-attacks has also increased proportionally. The data breach reports on various sectors were reported frequently in global as well as local medias. The patterns and methodologies used by hackers/attackers has also advanced and many of the organizations with complicated firewalls has compromised by these anonymous individuals. It's now become inevitable to protect the data and to secure them in this highly cyber infiltrated era.

Cybersecurity threats are estimated to cost the world US $6 trillion a year by 2021, and the number of attacks has increased five-fold after COVID-19[1]. The modern cyberattacks like DoS and DDoS attacks, MITM attacks, Phishing attacks, DNS Spoofing attacks has evolved during the time of pandemic and they have caused much more damage than their earlier interventions. Prevention and Counter Measures are the most important things that must be implemented in order to prevent these kind of data breaches and attacks. Prevention, Detection and Reaction are the 3 steps might help us guard against these attacks. Using the service of Certified personals who can perform Pen Testing on the databases can be a very effectful method. This paper is focused on pointing out the major reasons of increased cyber attacks in pandemic era. The intention is to light on the weaknesses and imbalances of current system and to provide a permanent solution for keeping the data secured.

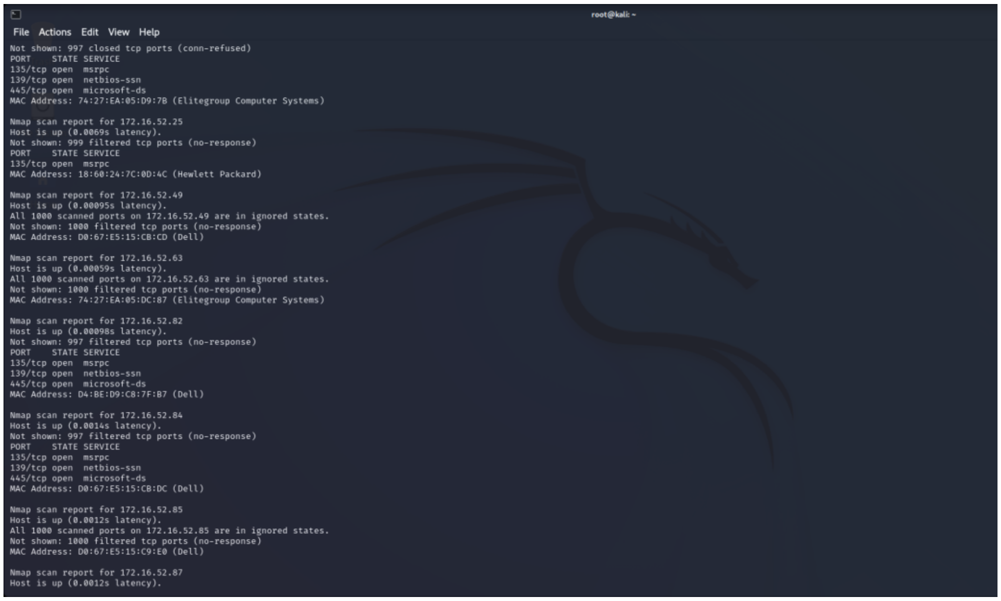
Existing System

The pandemic outbreak has caused a massive automation in world of internet. Day to day jobs have been automated using applications and websites. But this has caused a greater threat to the community in the form of cyber attacks. The fast automation has created many opportunities for the attackers to get their way into the databases and breach them. Studies show that the cyber attacks has increased 5 times in 2020 than that of in 2019.

1. Data of more than 530 million Facebook users, including their names, Facebook IDs, dates of birth, and relationship status, was published online in April 2021.
2. Dating app MeetMindful suffered a cybersecurity attack in January 2021, resulting in data of more than 2 million users being stolen and leaked. The hacking group behind the event managed to steal information like users' full names and Facebook account tokens.
3. One of the most damaging recent cyberattacks was a Microsoft Exchange server compromise that resulted in several zero-day vulnerabilities. The vulnerabilities, known as ProxyLogon and initially launched by the Hafnium hacking group, were first spotted by Microsoft in January and patched in March. However, more groups joined Hafnium in attacking unpatched systems, resulting in thousands of organizations being compromised.

[Source: https://www.fortinet.com/resources/cyberglossary/recent-cyber-attacks]

Its evident that the most complicated servers and infrastructures are no longer safer. Which means the local systems and networks are more under threat than anytime before.



```
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 74:27:EA:05:D9:7B (Elitegroup Computer Systems)

Nmap scan report for 172.16.52.25
Host is up (0.0069s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 18:60:24:7C:0D:4C (Hewlett Packard)

Nmap scan report for 172.16.52.49
Host is up (0.00095s latency).
All 1000 scanned ports on 172.16.52.49 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: D0:67:E5:15:CB:CD (Dell)

Nmap scan report for 172.16.52.63
Host is up (0.00059s latency).
All 1000 scanned ports on 172.16.52.63 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 74:27:EA:05:DC:87 (Elitegroup Computer Systems)

Nmap scan report for 172.16.52.82
Host is up (0.00098s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: D4:BE:D9:C8:7F:B7 (Dell)

Nmap scan report for 172.16.52.84
Host is up (0.0014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: D0:67:E5:15:CB:DC (Dell)

Nmap scan report for 172.16.52.85
Host is up (0.0012s latency).
All 1000 scanned ports on 172.16.52.85 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: D0:67:E5:15:C9:E0 (Dell)

Nmap scan report for 172.16.52.87
Host is up (0.0012s latency).
```

The above figure is the scan report of the devices connected to a certain subnet network. This shows that many of the connected systems has several services open and a technically skilled attacker can easily launch payloads through this open services.

Institutions like hospitals , colleges etc have huge databases containing the data of many people. This data is so vulnerable these days that we can see at least 1 news of data breach in any of these sectors. This paper is trying to point out the causes of this data breaches and it details the basics of cyber security mechanisms.

Proposed System

The proposed system is to effectively use the detection and prevention mechanisms available to prevent the cyber security issues facing by the current society. For that we have to understand about the hackers and the type of hackers.

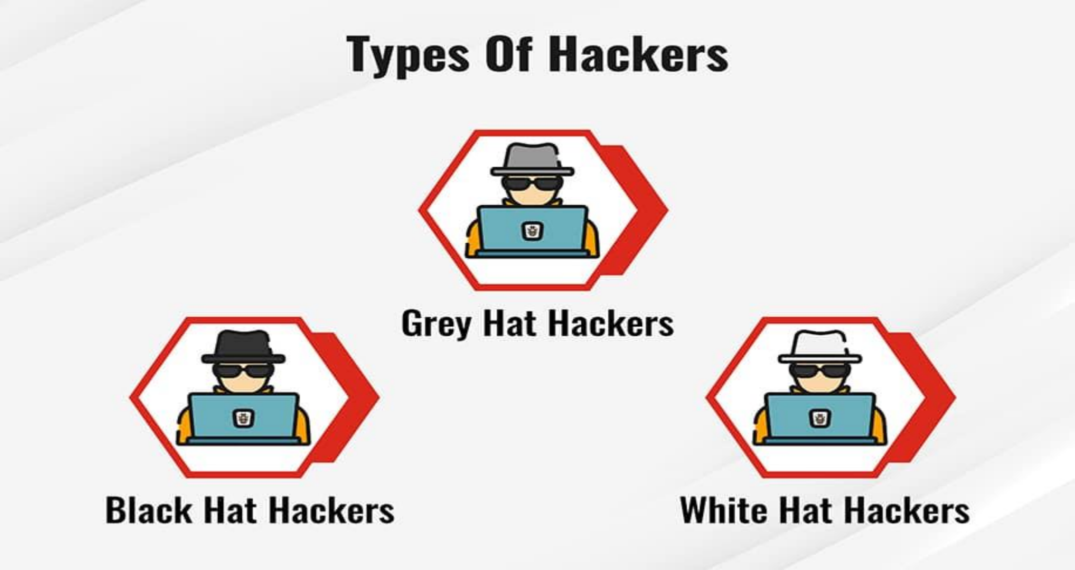
What is hacking?

Computer hacking is the act of changing computer equipment and programming to achieve an objective outside of the maker's unique reason.

Who is a hacker?

Hacker is a programmer who breaks into another person's computer framework or information without authorization.

Saying of the type of hackers they can be classified as the following



Source: https://marvel-b1-cdn.bc0a.com/f00000000216283/www.fortinet.com/content/fortinet-com/en_us/resources/cyberglossary/what-is-hacking/_jcr_content/par/c05_container_copy_c_501826447/par/c28_image_copy_copy_.img.jpg/1642017977242.jpg

Black Hat Hackers : They can be called as the bad guys in hacking. They finds out vulnerabilities and exploits them to gain access to the target and uses them for financial gain and malicious purposes, for gaining reputation etc.

White Hat Hackers: They are the good guys of hacking and they tries to protect the data from the attempts of the black hats using their own methods but in an authorized manner.They uses their technical skills to break into systems and check the security level to prevent from future attacks.

Grey Hat Hackers: They sits in between white and black hat hackers. Unlike black hat hackers they doesn’t use their skills to gain money or other personal benefits. They do breaks the rules and violates standard principles but they can be used for good purposes as well.

The idea put forwarded in this paper is to make maximum use of the White and Grey hats to prevent the attacks from black hats. Basically it is the idea of thinking like a hacker to prevent hacking. Nowadays many firms have cyber security wings for checking the safety of their data. But unlike these companies infrastructures like hospitals and educational institutions have data base managers only to manage their database. The major suggestion is to use the service of these white hats who are the legally qualified hackers to perform penetration testing on their systems. The advantage is that all possible vulnerabilities can be found by this and can be patched taking their advices.