A Comparative Study of Tools in Cybersecurity

Mrs. A.Regina Jayaseeli, M.C.A,M.Phil., HOD/Assistant Professor in Department of Computer science, Bishop Ambrose college, Coimbatore, Tamil Nadu

Mr.M.YUVARAJA, M.C.A., M.Phil., Assistant Professor in Department of Computer Science, Bishop Ambrose College, Coimbatore, Tamil Nadu

Abstract— This paper deals with cyber security tools which is trending currently. Corporate leaders wide viewed it because the responsibility of their IT department. Several thought -- maybe naively, it currently looks -- that farewell because the right firewalls, antivirus packages and secret writing tools were in situation, they might leave IT security to the specialists and specialize in the opposite myriad components of running a business, these kind of reasons bring forward to implement cyber tools for security. Few sectors like facebook, Equifax, The UK national Health Service also Yahoo had data breaches in recent years.

Keywords—Cyber, Bruteforce , Botnet

I. INTRODUCTION

Data protection and privacy stay the underlying problems that connect through the opposite sections. Even as technology is frequently progressing, the manner within which it’s used additionally changes and involves, that successively ends up in cybercriminals trying into new ways that to require advantage. Cyber security is that the combination of policies and practices to stop and monitor computer, networks, programs and information from unauthorized access or attacks that area unit aimed for exploitation. [1]Developing new ways in which to achieve unauthorized access to networks, programs and knowledge, attackers aim to compromise the confidentiality, integrity and handiness of data, building their targets from single people to little or medium sized firms and even business giants. each year looks to bring an even bigger variety of attacks overall, but also an even bigger variety of attacks affecting the protection of extraordinarily giant firms, therefore moving the data security, business continuity and customers’ trust. The increasing trend has reached new peaks in 2014, universally known as “the year of cyber-attacks”, however the authors believe this can be to not be the apogee unless countermeasures area unit taken at a world scale. this text has the aim of showing the results, trends and patterns noted by the authors through the analysis of the attacks reported within the last 3 years, and to gift countermeasures that ought to be taken as for supporting the development of security and therefore the decrease of world-wide cyber-crime. [2]. Security and value have usually been thought to be competitor system goals [6]. A classic example of the different aims of those 2 ideas is seen when coping with passwords, one amongst the foremost normally used security mechanisms nowadays. From a security perspective, long, advanced (hard to guess), distinctive passwords that area unit modified frequently is good, however, from a usability viewpoint, these needs area unit usually a significant strain on users and successively, a system’s usability. A majority of those general security problems are gift within the cybersecurity context, wherever the stress is on the digital surroundings. The challenge two-faced by the cybersecurity Usability and comparable Human-Computer Interaction and Security (HCISec/HCI-S) fields thus, is bridging that abstract and application gap, and emphasizing the need to fuse these 2 ideas thereby making usable cybersecurity interfaces and systems. this is often particularly as security measures and functions become customary parts in computer code applications and end-user systems. Common samples of these user-facing applications and systems embrace, data processing computer code (with tasks like adding digital signatures to facilitate future document authentication), document readers (which permit setting viewing, access and printing permissions), personal devices (with activities like applying security pins and
locks to mobile phones), personal security firewalls and email coding tools. All of those relate to typical tasks within the Net surroundings. The Internet of Things is the enabler of many applications, such as the smart home, smart cities, remote medical monitoring, and industrial control, by connecting a large number of sensors and actuators to the Internet. Existing studies predict that the number of connected devices will surpass 50 billion by 2020 [40].

II. CURRENT SCENARIO

The World Economic Forum’s international Risks Report 2019 stratified cyber attacks among the top ten most impactful international risks. A report revealed in 2019 by the Ponemon Institute shows that one in four network attacks could be a brute-force try. This attack used machine-controlled code to guess tens of or thousands of positive identification combos.

C. Browser Attacks:

These attacks target finish users World Health Organization square measure browsing the web. The attacks might encourage them to inadvertently transfer malware. These attacks used faux code update or application. Websites are force to transfer malware. The most effective ways in which to avoid browser-based network attacks is to often update net browsers.

D. Shellsock Attacks:

These attacks square measure refers to vulnerabilities found in Bash, a typical command-line shell for UNIX system and UNIX systems. Since several systems square measure ne'er updated, the vulnerabilities square measure still gift across the net. The matter is thus widespread that Shellshock is that the target of all networks.

E. SSL Attacks:

These attacks area unit intercept knowledge that's sent over associate degree encrypted association. These attacks with success access to the decrypted data. These attacks are quite common these days.

F. Backdoor Attacks:

These attacks square measure accustomed bypasses traditional authentication to permit remote access. These attacks square measure additional in software package deliberately. They have additional within the Programs or created by fixing associate existing program. Backdoors is a smaller amount common variety.

G. Botnet Attacks:

These attacks are hijackers. Computers that are controlled remotely by one or additional malicious actors. Attackers use botnets for malicious activity, or rent the botnet to perform malicious activity for others. Various computers may be caught during a botnet’s snare.

III. SECURITY ATTACKS AND TYPES

Security Attack is any action that compromises the safety of data owned by corporation victimization any method that designed to discover. There are many styles of attacks; however, commonest security attacks are delineated below [4]

A. Denial of Service:

These attacks are chiefly accustomed out of stock some resources sort of a internet server to users. These attacks are quite common nowadays. They used overload to resource with illegitimate requests for service. The resource cannot method the flood of requests and either slows or crashes.

B. Brute Force Attacks:

These attacks attempt to ruin the exterior door. It’s a trial-and-error arrange to guess a system’s positive identification. One in four network attacks could be a

Figure 1: Attacks perception ratio
The above figure depicts attacks vulnerability in cybersecurity. It shows prevention measures to be taken in order to secure data.

IV. CYBERSECURITY TOOLS

A Cyber Security code may be important for Cyber Security and Privacy of a business or individual. Cyber security is that the methodology that's accustomed shields the network, system, or applications from the cyber-attacks. It's accustomed avoid unauthorized knowledge access, cyber-attacks, and fraud.

Application security, data security, network security, disaster recovery, operational security, etc. are the various components of cyber security. It has to be maintained for numerous sorts of cyber threats like Ransomware, Malware, Social Engineering, and Phishing. [5]

Cyber Security Software can be categorized into different types as mentioned below:

- Network Security Monitoring tools
- Packet Sniffers
- Antivirus Software
- Encryption Tools
- Web Vulnerability Scanning tools

It provides a Cloud Archiving facility to firmly archive emails, files, and different information.

B. Tool 2- CIS:

CIS stands for the middle for net Security. It provides varied cyber security tools, services, and memberships. For business use, it provides CIS Secure Suite. CIS Security suite can embrace CIS controls and CIS Benchmarks.

Features:
CIS-CAT fatless performs an assessment automatically.
It provides 24*7 Security Operations Center and Incident Response Services.
It provides tools like CIS-CAT fatless, CIS-CAT professional, CIS bench, CIS RAM, and CIS CSAT.

C. Tool 3-Snort:

Snort is associate degree ASCII text file platform. It's associate degree application for network intrusion interference. It supports FreeBSD, Fedora, Centos, and Windows platform. It will perform the task of observance network packets and streaming information to your screen.

<table>
<thead>
<tr>
<th>S.no</th>
<th>Tool</th>
<th>Category</th>
<th>Feature</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mimecast</td>
<td>Email Security Tool</td>
<td>Cyber Resilience for Email as well as web</td>
<td>Business</td>
</tr>
<tr>
<td>2</td>
<td>CIS</td>
<td>Cybersecurity Tool</td>
<td>Tracing threats and securing platforms and also organization</td>
<td>Business</td>
</tr>
<tr>
<td>3</td>
<td>Snort</td>
<td>Intrusion Prevention Tool</td>
<td>Analyzing data packets in real-time</td>
<td>Business</td>
</tr>
<tr>
<td>4</td>
<td>Wireshark</td>
<td>Network Protocol Analyzer Tool</td>
<td>Decrypting protocols and inspecting many platforms</td>
<td>Commercial, Government Organizations</td>
</tr>
<tr>
<td>5</td>
<td>Webroot</td>
<td>End User Cybersecurity Tool</td>
<td>End user's real-time protection</td>
<td>Business and Home</td>
</tr>
</tbody>
</table>

- Network Defense Wireless Tools
- PKI Services

Table 1: Cybersecurity Tools Comparison

- Managed Detection Services
- Firewall
- Penetration Testing

A. Tool1-Mimecast:

Mimecast could be a cloud-based platform that gives email security and cyber resilience. It provides multiple product and services like Email security with threat protection, data protection, internet security, Cloud Archiving, etc.

Features:
Email Security with threat protection protects from spear-phishing, ransomware, impersonation and a few different sorts of targeted attacks.
It has options for machine-controlled Content management and information loss bar.
It provides net security by obstruction inappropriate business net sites and protective against user-initiated malicious web activity & malware.
E. Tool-5 Webroot:

Webroot may be a cloud-based platform. It will defend PCs, mackintosh computers, and mobile devices. It provides an answer for home use, home offices, businesses, and partners. It supports Windows, Mac, Android, and iOS platforms.

Features:

- Real-time protection against threat.
- Endpoints and networks are going to be protected with multi-vector protection.
- It provides cloud-based threat intelligence services.
- It offers prognostic threat intelligence.

V. CONCLUSION

The continuous innovations with various opportunities rendered by technology has conjointly got it reversed consequence, because the language goes, each have 2 sides either a head or a tail. This is often most evident because of the arrival of huge knowledge technology, cloud computing, automation and IoT. We have seen series of wave in cyber-attacks; state sponsored spying theme, cyber warfare, and cybercrimes. Therefore, nations round the world these days are concern regarding the way to secure and shield their national knowledge, either military or economically. Most tools are accessible to beat the protection problems few have been analyzed for simple use.

REFERENCES


