ISSN No:-2456-2165

Comparative Study of Various Open Source Cyber Security Tools

J. E. Peter
Department of ICT
Nigerian Navy Ship centenary
VI, Lagos State, Nigeria

R. I. Nwosu
Department of Computer Science
Federal College of Forestry Jos,
Plateau State, Nigeri

Abstract:- The invention of computing devices has brought higher attainment in professional and personal lives. Cybersecurity techniques is of growing importance due to increasing reliance on devices such as computer systems, smart phones, etc. which attempts to safeguard the cyber environment of users or organization . Cyber criminals aim at getting the information between a client and a server which are mostly in plain text formats through various means such as spreading malware inorder to gain unauthorized access. There is a need for users/organization to be aware of the various cyber-attacks and in order to prevent such attacks. This paper provides the various open source cybersecurity tools inorder to mitigate the different cyber-attacks.

Keywords:- *Open source, cybersecurity, cyber attack, cyber threats.*

I. INTRODUCTION

The world is in the so-called Information Age, characterized by rapid deployment of information and communication technologies [1]. Open Source Software is an integral part of the Information System and its applicable in entertainment and business domain [2]. The world has become smaller through the internet but it has also opened us up. As fast as security grew, the hacking world grew faster [3].

As technology evolves, cybercriminals also find new ways to take advantage of the loop holes in the new technology [4]. Cyber security combines both practices and policies to monitor computers, programs, networks, etc from attacks that is aimed for exploitation [5]. Attackers exploits ways to have unauthorized access to programs , networks, and knowledge for the aim of compromising the confidentiality and integrity of data[4]. Competitor system goals are security and value [6]. From security point of view, hard , long, and distinctive passwords is good, however, from a usability viewpoint, it is a constrain on users [4]. The challenges faced by the cybersecurity usability and Human-Computer Interaction and Security (HCISec/HCI-S) fields is bridging the application and abstract gap, thereby emphasizing the need to fuse both ideas by making usable cybersecurity systems and interfaces . This is common as security measures becomes ideal parts of computer code applications and end-user systems. Examples are data processing computer code , document readers, security firewalls, and email coding tools. Cyberthreat will continue to be on the rise as Internet of Things enables smart cities, smart home, remote medical monitoring, and industrial control. Existing studies predicted that the number of connected devices will surpass 50 billion by 2020 [7]. This paper focuses on the various open source cyber security tools with details of cybersecurity attacks. Table 1 shows cyber security tools, features, and application.

II. CYBERSECURITY

In a computing, security comprises of cyber security and physical security which are both used a measures against unauthorized access to data centre and other computerized systems inorder to maintain the integrity, confidentiality, and availability of data.

Security, access, integration of data, ,storage and transfer of data through electronic or other modes are measures for the concepts of cybersecurity [8]. Cybersecurity indicates three important factors which are methods of protecting Information Technology (data , data being processed and transmitted together with physical and virtual setup), the level of protection, and the professional aspects associated [9].

[10][11] defined cyber-security as a measure protecting computer systems, networks, and information from disruption or unauthorized access, use, disclosure, modification or destruction . [12] defined cyber security as the integration of policies, security measures, approaches to risk management, protocols, technologies, process and training which can be utilized in securing the organization and cyber setup along with user assets.

III. TYPES OF CYBERSECURITY ATTACKS

A. Denial of Service (DoS)

DoS attacks has becomed increasingly popular among attackers due to the growing number of IoT devices with insufficient security [13]. These attacks is quite common in which overload is used to flood the resource with illegitimate requests for service thereby slowing or crashing the network.

The sole objectives of DoS attack is to overwhelm the network with invalid requests which causes bandwidth wastage that result to lack of access to service by legitimate users . DDoS arises when a single target is attacked by multiple sources simultaneously which makes it difficult to identify and avoid. DDoS attacks occurs in variety of shapes and sizes, with the same purpose [14].

B. Man in the Middle (MiTM)

A type of MiTM attacks is Spoofing and impersonation. A MiTM attacker can pretend to be in a particular location while interacting with node Y . This attacker can establish a connection with the server through hypertext transfer protocol secure (HTTPS) while connecting with the victim over hypertext transfer protocol (HTTP) through secure sockets layer (SSL) stripping [13,15].

C. Malware

Malware (malicious software) application or script is intentionally designed to cause damage to networks ,computers, or data. An attacker can employ software patches to perform criminal operations and install malware. It comprises of worms, Trojan horses , spyware, rootkits, viruses, crimeware and other forms of deceptive advertising. These attackers are dangerous because they are well trained, state sponsored, and well funded[16].

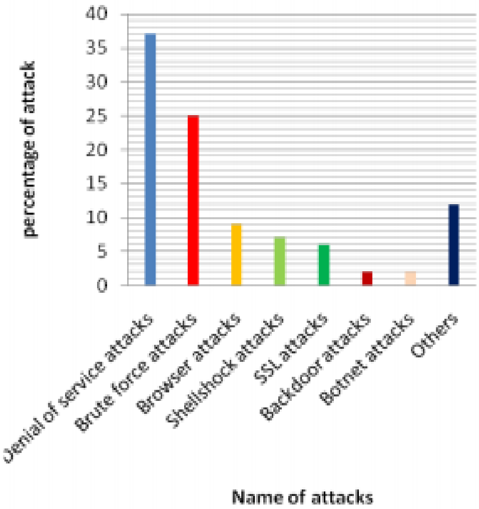

Fig. 1: Attacks perception ratio [4]

D. Botnet Attacks

Botnet attacks occurs when group of infected devices connects to the internet to engage in criminal and illegal activities together [17]. The affected computers are controlled remotely by one or more malicious actors.

E. Password Attack

The methods of password attack are dictionary and brute force method. Dictionary method decrypt an encrypted password while in brute force, multiple usernames and passwords are used [17]. These attack enable access to third parties passwords through malicious means.

F. Backdoor Attacks

Back door attack occurs when an attacker gains access to a website through a vulnerable entry point [18]. In distributed attacks, the surrounding network's infrastructure is affected but the specific server is not attacked.

G. Distributed Denial of Service attacks (DDoS)

In DDoS attacks, users are prevented from accessing network resources by over flooding the network with requests [17].

H. Spam attacks

Spam attacks use messaging systems to send messages which contain scams to a large number of target consumers. These messages are a source of phishing scheme [17].

I. Brute Force Attacks

This attack adopts trial-and-error approach to guess a system's positive identification. It uses machine-controlled code to guess positive identification combos [19].

J. Browser Attacks

This attack browser-based network attacks encourages the transfer of malware through websites but it can be avoided through regular update of the browsers [19].

IV. ROLES OF THE CYBERSECURITY FRAMEWORK

National and economic security requires cyber-security framework to help mitigate cyber hazards [20]. The cyber security framework defines an organization's best practices for managing cyber security risk in order to lower a company's vulnerability exposure. This framework document contains guidance that assist businesses in preventing and recovering from cyber-attacks [21]. The five primary roles of the cyber security framework are depicted in figure 2.

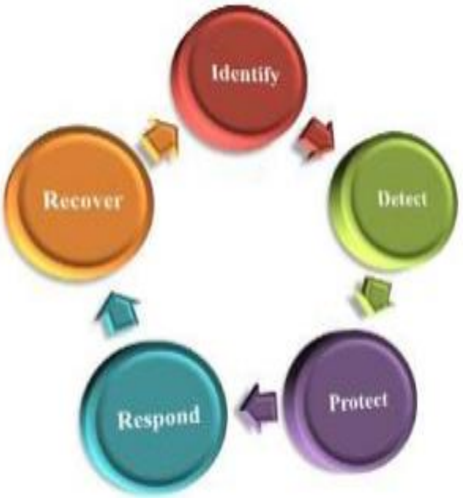

Fig. 2: primary roles of the cyber security framework [21]

- **Identify**: Companies must first understand their environments in order to manage cyber security risk on systems, data, assets, and capabilities.
- **Detect**: Procedures to detect cyber security incidents must be put in place by organizations.
- **Protect**: Suitable controls to limit or contain the consequences of potential cyber security incidents must be created and put in place by organizations.
- **Respond**: Reaction plans to mitigate the effects of cyber-attacks of businesses must be built.
- **Recover**: Effective strategies must be devised and implemented by businesses in order to restore capabilities or services that have been harmed as a result of cyber security incidents.

V. CYBERSECURITY OPEN SOURCE TOOLS

Various tools of data science can be employed by cybersecurity companies to process and analyze big data that are acting as a threat to intelligence data [22].

The Cybersecurity mechanism delivers a specific series of Free and Open Source Software (FOSS) and these cybersecurity devices are well ordered by functionality (Encryption, Anti-virus, Email Protection, Internet security, etc.) and unspecified target designs. The open source software tools may be free while analyzing FOSS but it's subject to source licensing constraints, and the free software tools might be free under closed source. The open source cybersecurity tools having thousands of security capabilities both defensive and offensively. Some of the significant security tools are being helpful to secure the systems and networks. The following are some of the open source security tools that have indispensable categorization due to the fact they are very productive, well sustain and it is easy to get start. Cybersecurity Analysts categorized their tools as follows: network security monitoring, encryption, web vulnerability, penetration testing, antivirus software, network intrusion detection, and packet sniffers [23].

A. Networking and Operating System Hardening

Hardening of the OS is the "act of configuring an OS securely, updating it, creating rules and policies to help govern the system in a secure manner, and removing unnecessary applications and services". Hardening is done to lessen the computer OS vulnerability to menace and to lighten viable risks.

a) OpenVPN
OpenVPN is freely available open source commercial software. It secures our data communications and produce adaptable VPN solutions . It provide solutions to the Cross-platform VPN clients and to VPN server and extend flexibility to site-to-cloud, users-to-cloud, site-to-site, devices-to-cloud, site-to-cloud and other network arrangements.

b) ModSecurity
ModSecurity is an open source application firewall. Sometimes it is called as ModSec. ModSecurity toolkit mainly useful in real-event web application logging, monitoring, and access control. ModSecurity acts as a module for Apache web servers and checks all HTTP requests that reach Apache and Nginx- supplementary web server of Apache.

c) SafePad
SafePad is an encrypted text editor. It mainly uses AES (Advanced Encryption Standard) encryption algorithm. SafePad is ideal editor for protecting the passwords, banking and card details and also providing secrets in big business.

B. Networking and Security Auditing

Network security auditing is a process for evaluating the effectiveness of a network's security measures against a known set of criteria. This audit looks at Hardware Configuration, Software Configuration, The Environment, Information Handling Processes and User Practices.

a) NMAP
NMAP stands for Network Mapper. It is a utility that provides information about the available ports (connection points) on the network. It has excellent OS and server software version detection. This tool analyzes IP packets of systems to gain information about the services running on the system, operating system, presence and type of firewalls, etc.

b) ZENMAP
Zenmap is an open source GUI invented to be utilized with Nmap. Zenmap is multi-platform tool which supports "Linux, Ubuntu, Mint, Kali, Fedora, CentOS, Windows, Mac OS X, BSD and so forth". Beginners can also use the Zenmap to discover vulnerabilities and to scan networks.

c) HPing
HPing is a "TCP/IP packet assembler/analyzer and furthermore a commandline oriented. It supports protocol like TCP, UDP, ICMP and RAW-IP. It has the mode called "traceroute" mode, which have the "capacity to send records between a secured channel, and numerous different highlights".

C. CyberSecurity Frameworks and Operating Systems

The cybersecurity framework makes our data and system safe. Habitually it in scripts the intention of overall security of an organization's moderately focusing especially on IT module. Most cybersecurity frameworks are intended to improve the existing security infrastructure already in place.

a) Kali Linux
Kali Linux is an operating system that is ready to go with every cybersecurity tool and capability needed to perform any kind of security work.

b) Qubes
Qubes is Free and Open Source Software (FOSS) operating system. It provides security by the utilization of compartmentalization in which the Components of the OS and apps are compartmentalized into qubes. Qubes allows for the running of Windows apps on Windows App Virtual Machines.

c) Metasploit
Metasploit is a popular tool used for penetration testing frameworks. It includes tons of exploits and payloads that can be used across all systems to gain access.

D. *Internet Security*

Typically, Internet security bounds with browser security, where secured data's invade through the Web form, and the Internet protocol sends the overall authentication and protection to the datas. Internet security is a boundless concern casing all the catch term security for transactions made over the Internet.

a) CheckShortURL
CheckShortURL is the cybersecurity tools used for checking shortened URLs . It supports almost all URL shortening services such as : "t.co, goo.gl, bit.ly, amzn.to, tinyurl.com, ow.ly, youtu.be and many others!".

b) NoScript
NoScript tool prevents falling victim to cross-site scripting and other types of script web attacks on Firefox and other Mozilla-based browsers. It additionally gives the most powerful anti-XSS and hostile to Click jacking assurance ever accessible in a program (browser).

E. *Email Security*

Email security empowers an independent or consortium to safeguard the comprehensive access to one or more accounts. It refers to the "collaborative measures used to secure the access and content of an email transcript".

a) SPAMfighter
SPAMfilter is an email security tool for filtering emails inorder to identify and stop spams.

b) Spamihilator
Spamihilator a security tool that determines spam emails using filters, a learning algorithm, and a probability calculator for email blockage.

c) SpamBully
SpamBully tool that learn and block spam using intelligent learning. It allows for spam reporting to fight back at spammers , auto delete options, etc.

F. *Password Management, Recovery and Attack Tools*

All sorts of business industries face a frequent challenge in password management. Most of the business industries uses unsecured spreadsheets and it still rely on paper based logbooks to manage their wealthy account credentials.

a) LastPass
LastPass ensures proper password practices as a foundation of security through the use of strong passwords.

b) KeePass
KeePass is a password management tool that helps to manage passwords in a closed way. By this, KeePass can put all passwords in a single database which is sealed under a single master key/key file.

c) Ophcrack
Ophcrack (GPL Licensed) is a graphical user interface tool that works by utilizing rainbow tables for password cracking in Windows OS. It is useful for recovering forgotten Windows passwords.

G. *Vulnerability Scanning Tools*

Vulnerability scanning plays a crucial role in IT security by scanning our websites and network from conflicting security risks and automates security audits. Vulnerability scanners are mastered in originating a prioritized list of patches, and also illustrate the vulnerabilities, anticipate steps on how to corrective them. It is also possible for some to even automate the patching process.

a) Burp Suite
The Enterprise Edition of Burp Suit performs carry out one-off scans on demand or schedule scans at precise time.

b) Nessus
Nessus is a vulnerability scanning tool that allows one to perform thorough scans of a network. Nessus home edition is free and takes up to 16 IP addresses.

c) Malwarebytes
Malwarebytes also called as MBAM (Malware Bytes Anti-Malware) - an antimalware software for macOS, Microsoft Windows, Android, and iOS ; it finds and removes unauthorized access.

VI. COMPARISON OF FOSS TOOLS

S/N	Tool	Features	Application
1	OpenVPN	-data communications secuurity - adaptable VPN solutions . -Cross-platform VPN clients and to VPN server -flexibility to site-to-cloud, users-to-cloud, site-to-site, devices-to-cloud, site-to-cloud and other network arrangements.	Commercial
2	ModSec	-real-event web application logging, monitoring, and access control. -it is a module for Apache web servers -it checks all HTTP requests that reach Apache and Nginx- supplementary web server for Apache.	Business and Home
3	SafePad	-text editor -uses AES (Advanced Encryption Standard) encryption algorithm.	Business
4	NMAP	-provides information about the available ports (connection points) on the network. -IP packets analyzer	Business
5	Zenmap	-multi-platform tool -use to discover vulnerabilities and scan networks	Business
6	HPing	-TCP/IP packet assembler/analyzer -supports protocols like TCP, UDP,etc –uses “traceroute” mode to send records between a secured channel and numerous different highlights	Commercial
7	Kali Linux	Tightly secured OS, with network services and other common services disabled by default, to minimize its visibility and attack surface.	Business and Home
8	Qubes	- security focused operating system. - It also allows the running of Windows apps on VMs.	Business
9	Metasploit	This is an exploitation and vulnerability validation tool you can use offensively to test your systems for known and open vulnerabilities.	Business
10	AdBlocker	block web requests that download content into the browser. allows you to browse the internet faster and without interruptions	Business and Home
11	CheckShortURL	reveals the destination of shortened URLs	Business and Home
12	NoScript	Allow potentially malicious web content to run only from sites you trust.	Business and Home
13	SPAMfighter	provides end-to-end solutions designed for Web App offers Anti Virus, Quarantine, Fraud Detection, Email Attachment Protection, Allow / Block List at one place.	Business and Home
14	Spamihilator	uses a number of filters to identify and weed out the spam	Business and Home
15	SpamBully	offers an efficient spam filter for your email client	Business and Home
16	LastPass	-The password manager supports 2-factor authentication methods -LastPass apps runs on cross platforms	Business and Home
17	KeePass	KeePass stores passwords in a secure database and unlocks by entering a single master key. It is powered by secure encryption algorithms such as: AES-256, ChaCha20 and Twofish and comes with complete database encryption;	Commercial
18	Ophcrack	-It comes with a Graphical User Interface and runs on multiple platforms. -Cracks LM and NTLM hashes	Business and Home
19	Burp Suite	intercept HTTP requests contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit	Commercial
20	Nessus	high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery and vulnerability analysis.	Commercial and Government Organisation
21	Malwarebytes	Anti-Malware. Detects and removes zero-hour and known Trojans, worms, adware, spyware, and other malware.	Business and Home

Table 1

VII. CONCLUSION

Cybercriminals have introduced different hacking techniques that makes individual and business sectors vulnerable to security problems. The various cybersecurity open source tools have been outlined in this paper to enable users to understand the possible threat and take required steps to safeguard the system and network.

REFERENCES

[1.] Barry M. Leiner at. al., “A Brief History of the Internet,” ACM SIGCOMM Computer Communication Review, Volume 39, Number 5, October 2009

[2.] Mihai DOINEA. Open Source Security Tools. Open Source Science Journal. Vol. 2, No. 2, 2010.pp 131-144

[3.] P.S.Seemma , S.Nandhini , M.Sowmiya . Overview of Cyber Security. International Journal of Advanced Research in Computer and Communication Engineering Vol. 7, Issue 11, November 2018. pp 125-128

[4.] A.Regina Jayaseeli & M.Yuvaraja (2020). A Comparative Study of Tools in Cybersecurity. Journal of Information and Computational Science. Volume 10(3), 580-584

[5.] J. Sherwood, A. Clark, and D. Lynas, Enterprise security architecture: a business-driven approach. CMP Books, 2005

[6.] K.-P. Yee, “Aligning security and usability,” Security & Privacy, vol. 2, no. 5, pp. 48–55, 2004.

[7.] U.Sinthuja, "A Study of IoT with Implementation and Testing Methods," ijrece, pp. 3379-3382, Apr-june 2019.

[8.] L. Bennett. Cyber security strategy. ITNOW, 54(1):10–11, 2012.

[9.] M. Qiu, L. Zhang, Z. Ming, Z. Chen, X. Qin, and L. Yang. Securityaware optimization for ubiquitous computing systems with SEAT graph approach. J. of Computer and Syst. Sci., 79(5):518–529, 2013

[10.] M. Gallaher, A. Link, and B. Rowe. Cyber Security: Economic Strategies and Public Policy Alternatives. Edward Elgar Publishing, 2008.

[11.] F. Pasqualetti, F. Dorfler, and F. Bullo. Attack detection and identification in cyber-physical systems. IEEE Transactions on Automatic Control, 58(11):2715–2729, 2013.

[12.] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. A survey on cyber security for smart grid communications. IEEE Communications Surveys & Tutorials, 14(4):998–1010, 2012.

[13.] Pfeiffer, A.; Gyulai, D.; Kádár, B.; Monostori, L. Manufacturing Lead Time Estimation with the Combination of Simulation andStatistical Learning Methods. Procedia CIRP 2016, 41, 75–80.

[14.] Barreno, M.; Nelson, B.; Sears, R.; Joseph, A.D.; Tygar, J.D. Can Machine Learning Be Secure? In Proceedings of the 2006 ACMSymposium on Information, computer and communications security—ASIACCS ‘06 2006, Taipei, Taiwan, 21–24 March 2006; pp. 16–25

[15.] Zhang, M.; Selic, B.; Ali, S.; Yue, T.; Okariz, O.; Norgren, R. Understanding Uncertainty in Cyber-Physical Systems: A ConceptualModel. In Proceedings of the European Conference on Modelling Foundations and Applications, Vienna, Austria, 6–7 July 2016; pp. 247–264.

[16.] Ning, Z.; Dong, P.; Wang, X.; Rodrigues, J.J.; Xia, F. Deep Reinforcement Learning for Vehicular Edge Computing. ACM Trans. Intell. Syst. Technol. 2019, 10, 1–24.

[17.] Goswami, G.; Agarwal, A.; Ratha, N.; Singh, R.; Vatsa, M. Detecting and Mitigating Adversarial Perturbations for Robust Face Recognition. Int. J. Comput. Vis. 2019, 127, 719–742.

[18.] Chaâri, R.; Ellouze, F.; Koubâa, A.; Qureshi, B.; Pereira, N.; Youssef, H.; Tovar, E. Cyber-Physical Systems Clouds: A Survey.Comput. Netw. 2016, 108, 260–278.

[19.] M. F. Theofanos and S. L. Pfleeger, “Guest editors’ introduction: Shouldn’t all security be usable?” IEEE Security and Privacy, vol. 9, pp. 12–17, 2011.

[20.] T. Chmielecki, P. Cholda, P. Pacyna, P. Potrawka, N. Rapacz, R. Stankiewicz, et al., "Enterpriseoriented cybersecurity management", Computer Science and Information Systems (FedCSIS) 2014 Federated Conference on, pp. 863-870, 7–10 Sept. 2014

[21.] Yusuf Perwej, Syed Qamar Abbas, Jai Pratap Dixit, Nikhat Akhtar, and Anurag Kumar Jaiswal . A Systematic Literature Review on the Cyber Security International Journal of Scientific Research and Management (IJSRM). Volume 09 Issue 12, Pages 669-710 .2021

[22.] Zhou, Y.; Han, M.; Liu, L.; He, J.S.; Wang, Y. Deep Learning Approach for Cyberattack Detection. In Proceedings of the IEEE INFOCOM 2018—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, USA, 15–19 April 2018; pp. 262–267

[23.] Balakrishnan Subramanian . An Overview List of Free Cybersecurity Tools. A Data Science Foundation White Paper, Atlantic Business Centre, Atlantic Street, Altrincham, WA14 5NQ. December 2019

[24.] Kaur, J., Kumar K.R, R., The Recent Trends in CyberSecurity: A Review, Journal of King Saud University - Computer and Information Sciences (2021), doi: https://doi.org/10.1016/j.jksuci.2021.01.018