International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Review on few cyber security tools

Sharanya K Rai[1], Rampur Srinath[2]

[1]M. Tech, Dept of ISE, National Institute of Engineering, Mysuru, Karnataka, India
[2]Associate Professor, Dept of ISE, National Institute of Engineering, Mysuru, Karnataka, India

---

Abstract - *A cyberattack is any type of attempt to destroy, uncover, change, disable, steal or gain unauthorized access to or make unauthorized use of an asset. Every year the number of cyber security attacks keeps on increasing. Hence there is a need for strong cyber security measures. Increase in the number of cyberattack is causing damage to companies, governments and individuals. Hence the organizations need to take proper measures to safeguard themselves against the attacks. In this paper I am presenting some cyber security tools which deals with some of the aspects such as malware attack, network security etc.*

***Key Words*: Eavesdropping, Network security, Traffic analysis, Intrusion detection, Brute-force attack, File encryption**

1. INTRODUCTION

Lack of information security gives rise to cybercrime. The increasing volume and sophistication of cyber security threats including targeting phishing scams, data theft, and other online vulnerabilities demand that we stay watchful about securing our systems and information. The average unprotected computer which does not have proper security controls in place when connected to the Internet can be compromised in moments. Thousands of infected web pages are being discovered every day. Hundreds of millions of records have been involved in data breaches. New attack methods are launched continuously. These are only a couple of cases of the dangers confronting us, and they highlight the significance of data security as a fundamental way to deal with securing information and systems.

1.1 Categories of Cybercrime

Based on the target of the crime cybercrime can be targeted against individuals, assets and organizations.

a) Crimes targeted at individuals: The goal is to exploit human weakness such as greed. These crimes include financial frauds, sale of non-existent or stolen items, child pornography, copyright violation etc.

b) Crimes targeted against property: This include stealing mobile devices such as cell phones, laptops, removal medias such as pen drives; transmitting harmful programs or malware that can disrupt functions of the systems and can wipe out the data from the hard disk and can create malfunctioning of the attached devices in the system such as modem, CD drive, etc.

c) Crimes targeted at organizations: Attackers use computer tools and the internet to steal the private information and also cause damage to the programs, files or some other data. Eavesdropping, Man in the middle attack are some of the attacks the cyber criminals do.

1.2 Need for cyber security

Unfortunately the cybercrimes are growing rapidly across the globe. Attackers make internet as a media to attack the system/data. With the development of the Internet, along came another revolution of wrongdoing where the culprits carry out acts of crime and wrongdoing on the World Wide Web. Internet crime takes many faces and is committed in diverse fashions. The eavesdropping of the data, injecting malware including virus, Trojan horses, etc. is done via internet.

Vulnerabilities are unfortunately an indispensable part of every software and hardware system. A bug in the operating system, a loophole in a code, or the misconfiguration of basic foundation components makes systems susceptible to attacks. Malicious techies can penetrate systems via these vulnerabilities, for personal or commercial gains. Hence, there is a crucial need for cyber security tools to safeguard the systems.

2. RESEARCH WORK

A. THE GNU PRIVACY GUARD

GnuPG is a free software used for email and file encryption. GnuPG allows encrypting and signing of the data and the mail, it also provides a flexible key management system. GnuPG, also known as GPG, is a command line tool with features for easy integration with other applications. An abundance of frontend applications are available belonging to one more following categories lists as follows: GUI frontends, MUA frontends, Chat programs, Network related, Frontends for scripting and many libraries such as Libgpg-error, Libgcrypt, Libassuan, Libksba are also available. GnuPG likewise offers support for S/MIME and Secure Shell (ssh).

GnuPG is a free software. It can be freely used, altered and distributed under the terms of the GNU public license. GnuPG is a hybrid-encryption software program since it uses a combination of conventional symmetric-key cryptography for speed and public-key cryptography for

simple secure key exchange, typically by using the recipient's public key to encrypt a session key which is used only once. GnuPG encrypts messages using asymmetric key pairs individually generated by GnuPG clients. The resulting public keys may be exchanged with other users in a variety of ways, such as Internet key servers. They must always be exchanged carefully to prevent identity spoofing by corrupting public key-owner identity correspondences. It is also possible to add a cryptographic digital signature to a message, so the message integrity and sender can be verified, if a specific correspondence depended upon has not been corrupted. GnuPG also supports symmetric encryption algorithms. By default, GnuPG uses the CAST5 symmetrical algorithm. GnuPG does not use patented or restricted software or algorithms. Rather, GnuPG uses a variety of other, non-patented algorithms.

GnuPG is a tool used to protect one's privacy. The privacy is protected if one user can communicate with others without a third person eavesdropping those messages. Customizing the use of GnuPG revolves around four issues:

- choosing the key size of the public/private keypair,
- protecting the private key,
- selecting expiration dates and using subkeys, and
- managing your web of trust.

A well-picked key size protects the user against brute-force attacks on encrypted messages. Securing the private key prevents an attacker from simply using the private key to decrypt encrypted messages and sign messages in the user's name. Accurately dealing with the user's web of trust prevents attackers from taking on the appearance of people with whom the user conveys.

B. Clam AntiVirus (ClamAV)

Clam AntiVirus (ClamAV) is a free, cross-platform and open-source antivirus software toolkit which scans a file for known viruses. ClamAV detects all forms of malware including Trojan horses, viruses, and worms, and it operates on all major file types including Windows, Linux, and Mac files, compressed files, executables, image files, Flash, PDF, and many others. ClamAV's Freshclam daemon automatically updates its malware signature database at scheduled intervals.

Clam Antivirus is an implementation of a virus scanner. The virus scanner consists of 2 parts: One is the actual scanner called as clamscan which scans a file to check whether it is infected with a known virus. It reports on the found viruses. The known viruses are kept in a database file. The second part called as freshclam serves to keep this database up-to-date: new viruses are born every day, and existing viruses change to more hazardous forms regularly, hence it is very important to keep the database with virus definitions up-to-date. The freshclam program should be run on a regular basis.

The unix version consists of client-server model where the scanner runs as a daemon. The clamscan program then sends the file to be scanned to the daemon, for inpection. This reduces startup time and system load, which is quite important on servers than run a heavyload MTA service. On Windows, a small GUI frontend exists which allows to perform and schedule scans, and to perform and schedule the virus database update. It does not have 'on-demand' scanning, i.e. scanning files as they are opened by programs. There is, however, a MS-Outlook plugin which can automatically scan attachments in emails. Also a context menu can be installed in the Windows explorer, which allows scanning of selected files straight from within the explorer. This should provide ample protection for most purposes.

C. OpenVAS

OpenVAS (Open Vulnerability Assessment System) is a framework which provides services and tools for intensive vulnerability scanning as well as vulnerability management. All of the OpenVAS products are free soft wares.

OpenVAS has SSL-secured service-oriented architecture. The core of this architecture is the OpenVAS Scanner. The scanner effectively executes the actual Network Vulnerability Tests which are served via the OpenVAS NVT Feed or via a commercial feed service. OpenVAS Scanner scans many target hosts are concurrently.

The OpenVAS Manager is the focal administration that consolidates plain vulnerability scanning into a full vulnerability management solution. The Manager controls the Scanner by means of OTP (OpenVAS Transfer Protocol) and itself offers the XML-based, stateless OpenVAS Management Protocol (OMP). OpenVAS Manager stops, pauses and resumes the scan tasks. There are different OMP clients which are available, hence the Green bone Security Assistant (GSA) is a lean web service which offers a user interface for web browsers. It gives multi-language support. GSA uses XSL transformation stylesheet to convert OMP responses into HTML. OpenVAS CLI contains the command line tool "omp" which allows creating the batch processes to drive OpenVAS Manager.

D. OSSIM (Open Source Security Information Management)

OSSIM (Open Source Security Information Management provides both security information management (SIM) and security event management (SEM) services integrating a selected tools intended to help network administrators in computer security, intrusion detection and prevention. OSSIM gives IT security experts the ability to cut through the noise in guarding and dealing with their systems. OSSIM consists of PRADS which is used to identify hosts and services by passively monitoring network traffic, OpenVAS, used for vulnerability assessment and for cross correlation of (Intrusion detection system (IDS) alerts vs Vulnerability Scanner) information.

E. Snort

Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system. It is capable of real-time traffic analysis and packet logging. It features rules based logging to perform content pattern matching and recognize a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, etc. Snort has real-time alerting capability, with alerts being sent to syslog, Server Message Block (SMB) ''WinPopup'' messages, or a separate ''alert'' file. Snort is configured using command line switches and optional Berkeley Packet Filter commands. The detection engine is programmed using a simple language that describes per packet tests and actions. Ease of use simplifies and speeds up the improvement of new exploit detection rules.

Snort inspects network traffic against a set of rules, and alerts administrators to suspicious network activity with the goal that they may respond suitably. Snort can be used to fill holes in commercial vendor 's network-based intrusion detection tools, such as when a new kind of attack in the hacker/cracker community and signature updates are slow to come from the vendor. In this case, Snort may be used to characterize the new attack by running it locally on a test network and determining its signature. Once the signature is written into a snort rule, the BPF command line filtering may be used to limit the traffic that Snort analyzes to the service or protocol of interest. Snort can be used as a very specialized detector for a single attack or family of attacks in this mode.

F. Security Onion

Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, and many other securitytools. Security Onion will provide visibility into the network traffic and context around alerts and anomalous events. Security onion provides mainly 3 functions:

- Full packet capture: Full-packet capture is accomplished via netsniff-ng "the packet sniffing beast". netsniff-ng captures all the traffic which the Security Onion sensors see and stores as much the storage solution will hold.
- Network-based and host-based intrusion detection systems (NIDS and HIDS, respectively): analyze network traffic or host systems, respectively, and provide log and alert data for detected events and activity.
- Powerful analysis tools: With full packet capture, IDS logs and Bro data, there is an overwhelming measure of information accessible at the analyst's fingertips. Security Onion incorporates the following tools to help understand this data: Sguil, Squert, Enterprise Log Search and Archive (ELSA).

G. Wireshark

Wireshark is a widely-used network protocol analyzer. It allows the user to see what is happening in the network. It is used for network troubleshooting, analysis, software and communications protocol development.

Wireshark can do a deep inspection of many protocols with more being added every time. It can live capture the data and then analyze them offline. Wireshark can also be used to capture packets from most network simulation tools such as ns, OPNET Modeler and NetSim. Wireshark runs on many platforms such as Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, etc.

It has the most powerful display filters. The user typically sees packets highlighted in green, blue, and black. Wireshark uses colors to help the user identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order. Users can change existing rules for coloring packets, add new rules, or remove rules.

H. ProofPoint

Proofpoint is the best security tool for detecting attack vectors or holes in the security system where cybercriminals can get in. It focuses on email with cloud only services for all companies, regardless of their size. This security tool also protects outgoing data and stores data to prevent its loss. It does not use keys to decrypt any of the data.

Proofpoint's security portfolio includes products that stop both traditional cyberattacks (delivered via malicious attachments and URLs) and socially engineered attacks—such as business email compromise (BEC) and credential phishing—that do not use malware. It uses a blend of sandbox analysis, reputational analysis, automated threat data, human threat intelligence and attributes such as sender/recipient relationship, headers, and content, and more to detect potential threats. Automated encryption, data-loss prevention and forensics-gathering tools are designed to speed incident response and mitigate the damage and costs of any threats that do get through. The portfolio also includes protection from social-media account takeovers, harmful mobile apps, and rogue Wi-Fi networks.

3. SUMMARY

As discussed above the GNU privacy guard is used for email and file encryption to avoid man in the middle attacks, eavesdropping, etc. It protects one's privacy. The Clam Antivirus (ClamAV) scans file for known viruses including Trojan horses, viruses, and worms on almost all major file types. OpenVAS does an intensive vulnerability scanning as well as vulnerability management. OSSIM provides security information management and security event management. Snort can be used to detect denial of

service attack. Another application to which Snort is very well suited is as a Honeypot monitor. Honeypots are programs or computers that are dedicated to the notion of deceiving hostile parties interested in a network. Security Onion will provide visibility into the network traffic and context around alerts and anomalous events. Wireshark is used for network troubleshooting, analysis, software and communications protocol development. Proofpoint detects attack vectors or holes in the security system from which the cybercriminals can get in and attack.

4. CONCLUSIONS

In this paper we have discussed some of the main tools to fight against the cyberattacks. We hope in future more powerful and effective tools and techniques emerge to prevent cyberattacks.

REFERENCES

[1] http://ranger.uta.edu/~dliu/courses/cse6392-ids-spring2007/papers/USENIXLISA99-Snort.pdf
[2] http://www.admin-magazine.com/Archive/2014/20/Open-Source-Security-Information-and-Event-Management-system
[3] https://www.educba.com/32-most-important-cyber-security-tools/
[4] Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives by Nina Godbole and Sunit Belapure
[5] https://github.com/Security-Onion-Solutions/security-onion/wiki/IntroductionToSecurityOnion
[6] https://securityonion.net/
[7] https://en.wikipedia.org/wiki/Wireshark
[8] https://en.wikipedia.org/wiki/Proofpoint,_Inc.
[9] https://gnupg.org/index.html
[10] https://www.gnupg.org/gph/en/manual.pdf
[11] https://www.clamav.net/