International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT206391

Digital Auditing: A Technique to Ensure Security

Nidhi Dandotiya*[1], Dr. Pallavi Khatri[2], Abhinandan Singh Dandotiya[3]
*[1]CSA Department, ITM University, Gwalior, Madhya Pradesh, India
[2]CSA Department, ITM University, Gwalior, Madhya Pradesh, India
[3]CS&A Department, Shri Krishna University, Chhatarpur, Madhya Pradesh, India

ABSTRACT

Security is one of the ever-rising provinces in about every field of society and computers are no freak. The system on the network can be attacked if it is easy to break its security or it is vulnerable. Security issues that exist in connection to a machine on network are system security and application security. For ensuring security of personal computer regular security audits of the system needs to be done. One main objective of auditing is to ensure that systems are safe or not. Digital auditing can be manual or automated. Systems audit leads to check that the vulnerability of system to different attacks that can be done on it. Similarly, a website running on the system can also be exploited for any vulnerability in it. This work investigates the methods of system and application auditing to identify the weakness at system and application level.

Keywords : Forensic Investigation, RAM, Security, Window auditing, website auditing

I. INTRODUCTION

A complete computer system security planning should not involve only policies and procedures that ensures the rights to access the system are configured for each user, rather it should also for verify these rights. The system must have capabilities to keep this check on all the deployed rules for system access over the network. Being able to understand what our network users are doing proves to be an effective method of monitoring the systems over the network. System auditing is a method for acquiring information concerning how powerful your security exercises are. System auditing is a procedure for tracking events, perceiving where and when these events comes up and who initiate them. It can help to perform forensics investigation. This could be helpful to detect problems such as unethical rights assignments in the file system. The system audit policies define the specific events that one logged, and what exact behaviors are logged for all events. These logs can be use by a forensic expert while doing a forensic investigation in case of any crime reported. System audit is the process of tracking analyzing, and understanding events that take place on computer systems. System audit can recognize steps to upgrade security management and reduce the chance of uncertified access and unwanted changes to your systems. Application audit is also very useful for application developers because application can be checked for traffic goals, its performance vulnerability etc. Application auditing is a full analysis of all vulnerable factors that can affect the system. These vulnerabilities reported can be used to enhance the security features of the application. This study outlines various methods that can be used to secure a system that is running a windows operating system and under application security website audit has been taken up.

In this paper section 1 will give a brief description of security audit system for compliance so as to fulfill

requirement. Section 2 will share some related work and section 3 will introduce the description of digital forensics. Section 4 presents the methodologies of audit. in last we concludes the overall work.

II. RELATED WORK

Digital forensics becoming very important process to inquire computer and cyber assisted crime [1]. Cyber crimes are increasing enormously and a procedure for effective and efficient examination of the systems involved in crime should be in place so as to help the cyber forensic experts. In last decade, a paradigm shift has been noticed in the volume of work and data in digital world. As the volume increased, speed came up as a challenge and quick access to data became the need. Large volumes of data stored on third party domains posed a threat on security. All these issues made it difficult for the stakeholders to keep up with CIA (Confidentiality, Integrity, and Authenticity) triad. Settings of operating system allow setting up the group policies for the users of the system and multiple security settings can also be configured. Without setting up these policies of OS (Operating System), it is difficult to achieve security as per CIA triad and more difficult to stop and trace the crimes done through digital devices [2]. The main aim of security framework is to monitor and manage the system security and audit information [3]. The framework as discussed in [4] aims to help the organizations to know what exactly is required to protect their digital repositories and what are the vulnerabilities that enable to deploy a feasible solution for security management. IT security audit accumulates, assesses, and tests the data of an organization's systems, and determines that systems are safeguarding the data, managing data integrity, and are effectively handled to attain the organization's business objectives [5]. Web based applications are widely exposed and available over internet. Any application vulnerability can easily be discovered by bad guys in the network and can lead to exploit machines on the network through web applications. Web developers needs to implement best coding techniques and should perform security checks through PT (Penetration Testing) and using code vulnerability analysers before deploying the web applications [6].

This work has taken up the study on computer & web application forensics. This work aims to focus on the importance of windows and web forensic analysis. Experiments done try to extract and analyse all information that can lead to conclusions for a forensic investigator. Entries of Windows registry are used for forensic analysis of a system involved in any crime. This work focuses on forensic analysis of a machine running windows 7 operating system. Main target of the work is to identify an illegitimate login to the machine and copying of file on an external USB drives. This is tracked by checking the modified registry key values.

III. WHAT IS DIGITAL FORENSIC

Digital Forensics is a process of identifying and extracting the digital evidences from a digital device involved in cyber crime and preserving the digital evidence to be presented in the court of law. Field of digital forensics equips a cyber forensic expert with the tools and techniques to carry out the forensic analysis of digital evidence and to extract important artifacts from it in case of any digital crime committed from a device. It also supports the forensic team with a clear protocol to carry out the cyber investigation. Following steps needs to be followed by a cyber forensic expert while carrying out a forensic investigation:

Identification: This step includes identification of the digital device, its serial number, place, date, time, users of the device, external devices connected evidence that can be collected.

Preservation: This step leads to make multiple clones / images of the storage of the digital device on which investigation needs to be performed and then preserving the original device so as to stop any tampering in the data.

Analysis: In this phase, cyber investigator analyzes and reconstructs the data that can lead to some conclusion related to the reported case. Every finding is recorded in documents to be presented in court of law.

Documentation: This step follows the identification phase. A chain of custody document is prepared in this phase. Every detail of all hardware, software, users present on the crime scene is recorded in this document with exact date and time. This document if presented to the court of law at the time of hearing. It is supported with crime scene photographs, sketches etc.

Presentation: This step summarizes the investigation process and also the conclusion drawn from it. This document is prepared in exceedingly layperson's terms with are the references clearly made.

IV. METHODOLOGY

In this research two experiments has been performed one for windows system and other for website audit.

Experiment 1: Windows Audit

Window auditing can be done using either manual or automated method.

Manual method - Auditing can be done with the help of command prompt. Follow the steps given below for window auditing open command prompt as administrator type command secpol.msc Secpol command is used for open local security policies and msc is another windows module that is also used for administration of system settings. After executing this command local security policy window is open and (that is shown fig-1).

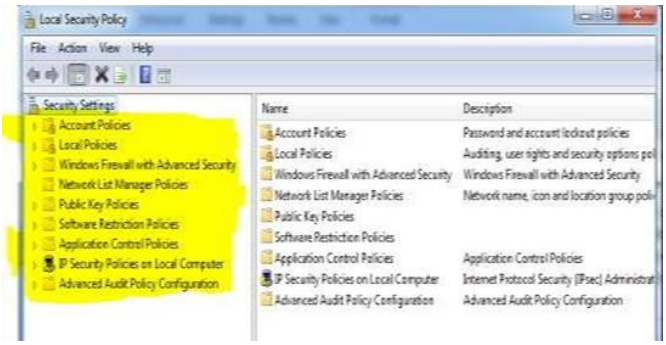


Fig 1. Windows Security Policies

Local Security Policy in Windows allows enforcing many systems as user and security-related settings, like password policy, audit policy and user permissions. Event Viewer can check log events.

When local security policies windows open then there is following nine options available and these options provide the detail of the whole system for instance-

i- Account policies. ii- Local policies.

ii- Windows firewall with advance security

iii- Network list manager policies. v- Public key policies.

iv- vi- Software restriction policies. vii- Application control policies.

v- IP security policies on local computer. ix- Advance audit policy configuration.

By default, in windows most policy settings are fine, but a couple of most significant ones despite all needs modifying for upgraded security.

(i). Password Policies – account policies give the detail of password policy. This section gives the detail and also set some criteria (that is shown in fig-

2) of the system password. The password policies provide a way to organizations to define different password and account lockout policies to different

sets of users in single domain. Fine-grained password policies apply only for user objects and global security groups. These policies incorporate attributes of all settings that can define in default domain policy also account lockout settings. Only individual members of Domain Admins group can set fine- grained password policies. The User can impose the use of strong passwords through an suitable password policy.

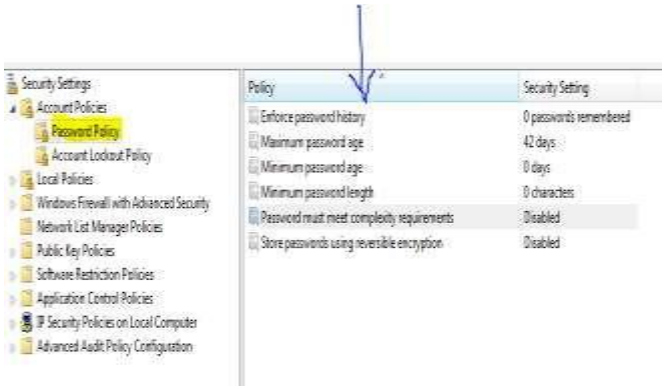


Fig 2. Windows Password Policy

(ii). Local Policies- local policies have three subsection audit policies, User right assignment, and security options. In the audit policy section you get the nine sort of auditing options available.

Account Logon Events: In this segment, the auditor can check track login, logouts and connections detail.

Account Management: In this segment, the auditor can assess changes in track accounts

Directory Service Access: In this segment, the auditor can check tracks access and the directory services which is active.

Logon Events: logon events also have details of track logins, logouts, and details of connections.

Object Access: object access keeps the detail of accessing tracks of files, directories and the NTFS objects.(everything in windows including printers is consider as an object)

Policy Change: It can tracks changes to user authority, trust , and audit laws.

Privilege Use: in this section, we can change the tracks user preferences.

Process Tracking: this section can activate and terminate the track program

System Events: In this event the tracks server goes shutdowns and then restart. This log events affecting system policy

(iii). Window firewall with advance security- this section provides network security for window computers.

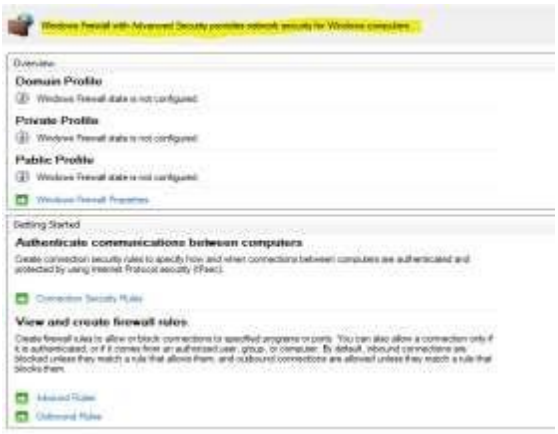


Fig-3 Window Firewall with advance security

(a) ***Windows audit (automated)-***

In this experiment, auditing is done with the help of a win audit tool. This tool automatically generates an audit report as shown in figure. Win Audit is a utility for Windows PCs. It makes a complete report on a machine's configuration and programs. Win Audit is a free, open-source and can be utilized or shared by anybody. It is utilized by IT specialists in the scholarly community, government, industry along with security cognizant experts in the military services, defense contractors, power generators and police department.

Fig-4 Audit Report Generate by Software

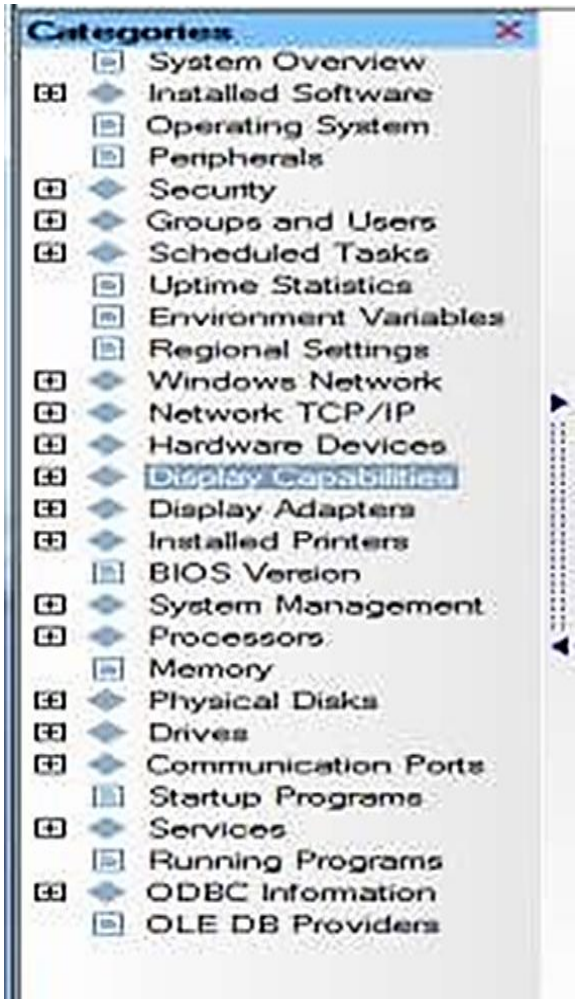


Fig-5 Categories in Win audit Report

Audit Report

An audit report generated win audit tool is used by forensic investiger to fill in the check list as shown in below table.

S.No.	Domains	Remarks
1.	Account	
(a)	System Installation date	
(b)	Separate user account with standard privilege only?	
(c)	Administrative (installed) account renamed?	
(d)	Does User know administrator account password?	
(e)	Guest account enabled?	
2.	Patch Management	
□	Latest Update date?	
3.	Three Layer Password	
□	Password implemented on BIOS?	
	Password implemented on OS?	
	Password implemented on screen saver?	
4.	Security Settings	
(a)	Password policy configured?	
(b)	Account lockout policy configured?	
5.	Antivirus Firewall	
	Antivirus installed?	
	Antivirus Last Scanned?	
	Antivirus Last Updated?	
	Firewall enabled?	
6.	External media Usage	
	Does user use pen drive /external HD in computer?	
	Does user connect mobile phone /camera in PC?	
	Does user use internet dongles in PC?	
7.	Other security Settings	

	Remote Desktop enbled?	
	Auto play at devices enabled?	
	SSH root login disabled?	
	IPV6 Disabled	
	IP spoofing prevented	
	Any add on in browsre	
	SYN attacks blocked?	
8.	Audit Policy	
	AUDITO Service installed?	
	Audit log size?	
	Login and logout event recorede?	
9.	MISC	
	Clear Desk & clear screen	
	Suspicious links found in browser history?	

Audit checklist is a document that can be produced in court of law. This is always filled at the time of seizing the system.

Experiment No. 2: Website Audit

This section presents how website auditing works. Website auditing is required for finding web vulnerability. Website vulnerability means weakness and mis-configuration of website and also website application code is written in a weak format that allows to attacker gain some level of control in the website. Knowing these vulnerabilities can be harmful to any organization. In web site auditing whole web site would be scanned with the tools. This audit uses Nessus and Acunetix for finding the website vulnerabilities.

Scanning information using Nessus Tool-

Nessus is a GUI based tool this allows to scan the environment with the high speed and depth assessment. For scanning a website in nessus first select the new scan and give target website then start scanning.

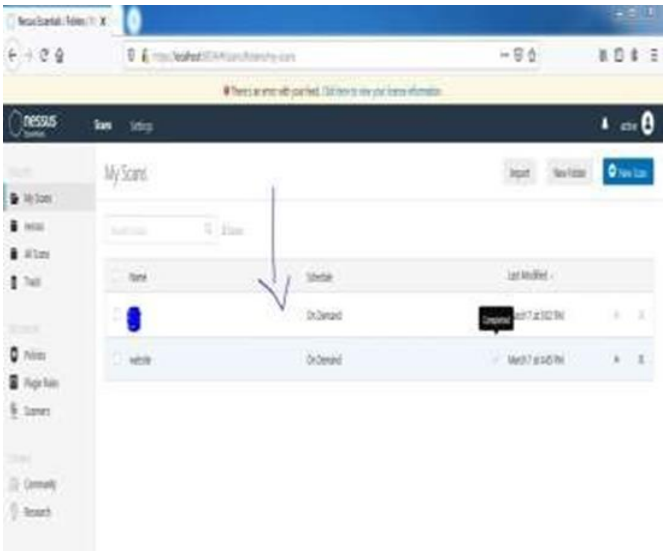
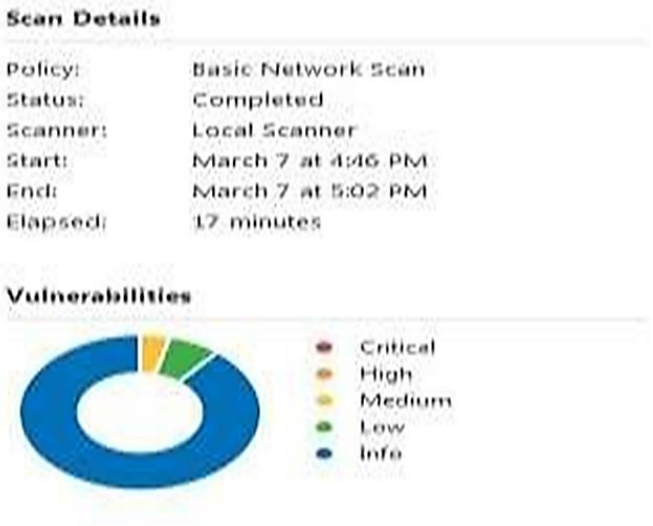


Figure-6 Start New Scan in Nessus

Website scanning takes some time. After complete scanning, Nessus gives scanning results as shown in (Fig-7). All vulnerabilities details of a website are listed in the scan results.



Figur-7 Vulnerabilities Detail showing in Pie Chart

In this detail (FIG-7) scanner gives the scanning start and end time and also give completion time of scanning. Nessus also give detail description of vulnerabilities as shown in Fig-8.

Figure-8 Vulnerabilities Detail 1

In the above figure, there are 23 vulnerabilities found and colors describe the vulnerability level. The yellow denotes medium, green denotes low, and blue denotes just a information that is not providing so much harm of website. Click on this section that give much detail about vulnerability.(Fig-9)

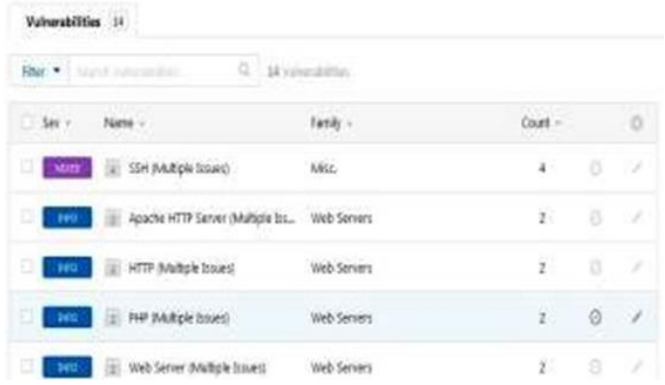


Figure-9 Vulnerabilities Detail 2

In the above figure, one mixed SSH vulnerability found this SSH called secure shell vulnerability. This vulnerability allow authentication without a password. After found this vulnerability, If click on mixed (means more than one vulnerability combine but all are SSH vulnerability) then see the proper detail this vulnerability (Fig-10) and if click on medium (yellow section) than see the whole detail about this vulnerability also check how this vulnerability fix. (Fig 11)

Figure-10 Vulnerabilities Detail 3

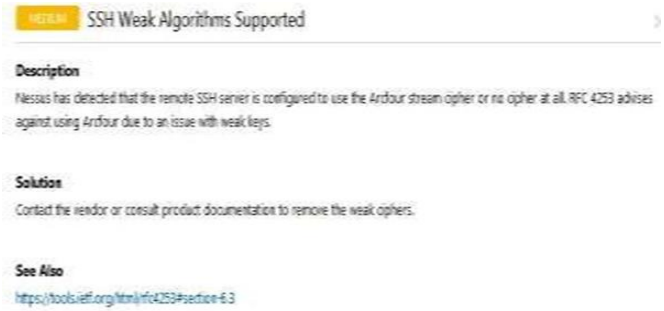


Figure-11 Vulnerabilities Detail 4

2.2 Scanning information using Acunetix Tool- Acunetix is a web vulnerabilities scanner. This tool can scan any web site. For scanning the website first give URL of target website and start scanning. After some time that gives some detail (Fig -12)

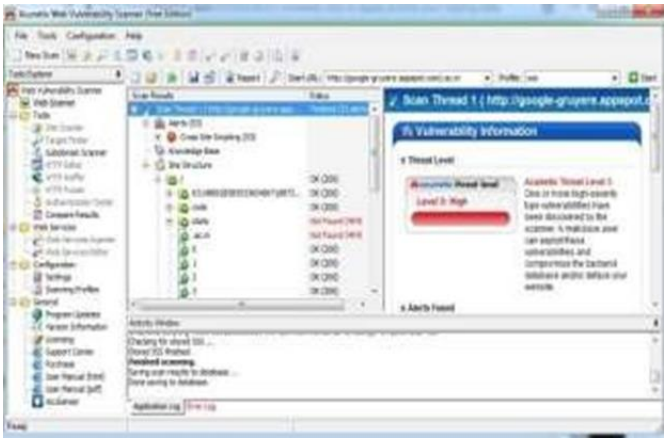


Figure-12 Scanning on Acunetix

When scanning complete that give scan result (Fig 13) that provide the detail how much and which type vulnerability found in this website, as in Fig 13 can see that only 53 cross site scripting vulnerability found and this scanning also provide vulnerability information in the form of high, medium, low etc. format (Fig 14).

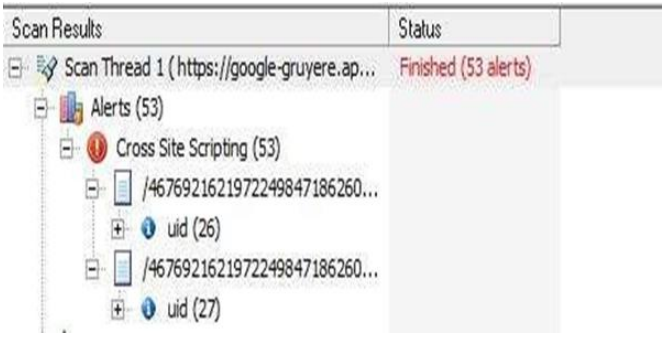


Figure-13 Scan Result

Figure-14 vulnerabilities Information

Figure-15 Scanning Information

When scanning a website through this scanner that gives 53 high vulnerability of this website and also provides scanning information (Fig-12) of this website. The scanner gives detail portrayal of vulnerability (Fig- 13). This website find many cross site scripting vulnerabilities, through this scripting malicious script is injected and this tool gives the vulnerabilities name and detail description of the vulnerability and also tell that which item is affected through this vulnerability and solution of this (Fig-13 and 14).

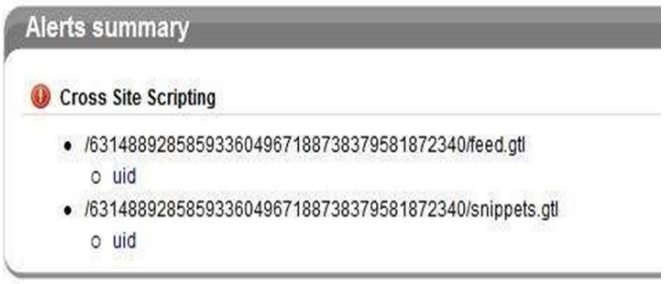


Figure-16 Vulnerabilities Name

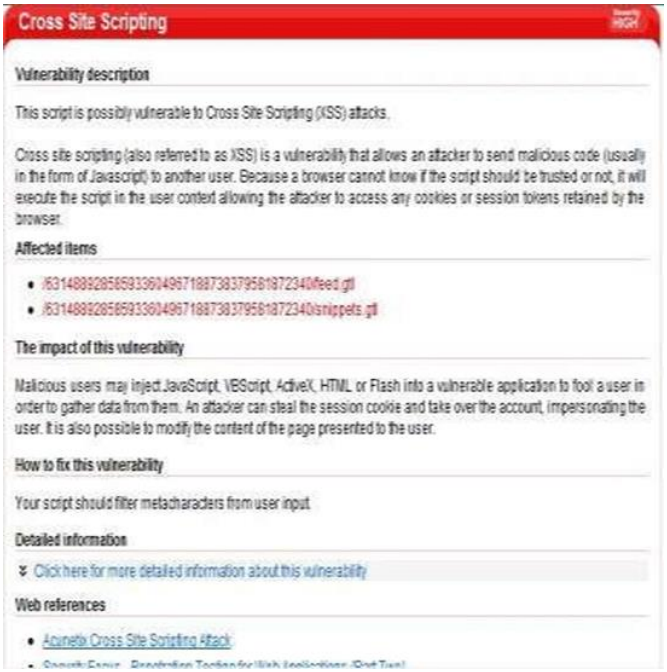


Figure-17 Vulnerabilities detail description

If the coder gets to know this information then the coder can change the website code and remove these vulnerabilities form website. This scanner can check any of the web site vulnerabilities information and also find how to fix these vulnerabilities.

V. CONCLUSION

Overseeing assaults and dangers which the data arrangement of the associations are subject of, is progressively troublesome, because of the characteristic develop of the assaults, dangers and Vulnerabilities, advanced by the advances of innovation. The fundamental commitment of this paper is to understand and managing security tools of systems, for the vulnerabilities of system and applications.This work describes different methods

and tools of application and systems audit. Applications and systems editors are continue working with different available tools of scanning and auditing to secure the data. System audit is required to secure the system from vulnerabilities.

VI. REFERENCES

[1]. M. Al Fahdi, N.L. Clarke , S.M. Furnell," Challenges to Digital Forensics: A Survey of Researchers & Practitioners Attitudes and Opinions", International Conference Information Security for South Africa 2013

[2]. Abhijeet Ramani, Somesh Kumar Dewangan ,"Digital Forensic Identification, Collection, Examination and Decoding of Windows Registry Keys for Discovering User Activities Patterns", International Journal of Computer Trends and Technology (IJCTT) Nov 2014, vol. 17 no. 2

[3]. Abhijeet Ramani, Somesh Kumar Dewangan,"Auditing Windows 7 Registry Keys to track the traces left out in copying files from system to external USB Device", International Journal of Computer Science and Information Technologies(IJCSIT), 2014 vol. 5 no. 2, pp.1045-1052

[4]. Teresa Pereira , Henrique Santos," A Security Audit Framework to Manage Information System Security", International Conference on Global Security, Safety, and Sustainability ICGS3 2010

[5]. Jungwoo Ryoo , Syed Rizvi, William Aiken , John Kissell "Cloud Security Auditing: Challenges and Emerging Approaches" Digital Object Indentifier 2013 10.1109/MSP.2013.132 1540-7993 IEEE

[6]. Marco Vieira, Nuno Antunes, Henrique Madeira," Using Web Security Scanners to Detect Vulnerabilities in Web Services", IEEE/IFIP International Conference on Dependable Systems & Networks 2009

[7]. Meiko Jensen · Nils Gruschka · Ralph Herkenhoner," A survey of attacks on web services Classification and countermeasures.", Springer-Verlag 2009

[8]. Nilay R. Mistry , M. S. Dahiya" Signature based volatile memory forensics: a detection based approach for analyzing sophisticated cyber attacks",An Official Journal of Bharati Vidyapeeth's Institute of Computer Applications and Management 2018

[9]. online]Available: thttps://www.beyondtrustcom/resources/glossary/windows- auditing

[10]. Online]Available: https://www.petri.com/windows_ auditing

Cite this article as :

Nidhi Dandotiya, Dr. Pallavi Khatri, Abhinandan Singh Dandotiya, "Digital Auditing: A Technique to Ensure Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6, Issue 3, pp.371-379, May-June-2020.
Available at
doi : https://doi.org/10.32628/CSEIT206391
Journal URL : http://ijsrcseit.com/CSEIT206391