Sufficiency of Windows Event log as Evidence in Digital Forensics

Nurdeen M. Ibrahim & A. Al-Nemrat, Hamid Jahankhani, R. Bashroush

University of East London
School of Computing, IT and Engineering, UK
u0947707@uel.ac.uk;{ameer; hamid2; rabih@uel.ac.uk}

Abstract. The prevalence of computer and the internet has brought forth the increasing spate of cybercrime activities; hence the need for evidence to attribute a crime to a suspect. The research therefore, centres on evidence, the legal standards applied to digital evidence presented in court and the main sources of evidence in the Windows operating system, such as the Registry, slack space and the Windows event log. In order to achieve the main aim of this research, cybercrime activities such as automated password guessing attack and hacking was emulated on to a Windows operating system within a virtual network environment set up using VMware workstation. After the attack the event logs on the victim system was analysed and assessed for its admissibility (evidence must conform to certain legal rules), and weight (evidence must convince the court that the accused committed the crime).

Keywords: Cybercrime; Digital forensics; Digital evidences

1 Introduction

The proliferation of computer and network systems has brought forth the increasing spate of cyber crime (Wang, 2006). The Windows operating system is the most prevalent; therefore, Windows users bear the brunt of most cyber crimes (Dashora et al., 2010). Criminals constantly devise a variety of technique to perpetrate crime; and are constantly updating their skills subsequently, the need for measures to investigate how computer crimes are committed and mechanisms for identifying suspects, in order to present evidence needed for successful prosecution is vital to mitigating cyber crime. The need for technology to combat cyber crime has therefore conceived computer forensics (Wang, Cannady and Rosenbluth, 2005). "Computer forensics can be summarised as the process of collecting preserving, analysing and presenting the computer-related evidence in a manner that is legally acceptable in court" (Abdullah et al. 2008, pp.215). Evidences gathered during forensic investigation could be used in criminal cases such as in intellectual property theft and other civil cases.

However, for evidence to be admitted in court it has to satisfy two test which is the admissibility (evidence must conform to certain legal rules) and weight (evidence should sufficiently convince the court that the crime is committed by the accused). The admissibility test requires that evidence conform to certain legal rules such as authenticity and reliability, best evidence rule and hearsay rule (Sommer, 1999). After evidence is admitted in court, its weight is assessed to determine its probative value (Casey, 2004). The Windows operating system preserves a pool of data from which investigators can obtain evidence pertinent to a case under investigation (StrathclydeForensics, n.d.). Evidence related to cybercrime activities can be found locations such as, Registry, Slack space and the Windows event log (Steel, 2006).

The Windows event log is the most important source of evidence during digital forensic investigation of a Windows system because the log files connect certain events to a particular point in time (Schuster, 2007). An

event in Windows Event log is an entity that describes some interesting occurrence in a computer system (Stallings and Brown, 2008, pp. 486). For instance event log is generated when an operating system starts, stops or fails, when a user attempts to access system resource or logged on to a computer etc. To the digital forensic investigator event logs is of enormous benefit as it provides a detailed step by step account of activities that occurred in a system. By investigating the event logs incidence response team could tell whether an attempt to intrude a system succeeded or not. (Vivienne and Sutherland, 2005).

The objective of any investigation is to identify evidence that is needed to attribute a crime to the perpetrator. This can be achieved by unveiling information that links a crime to a suspect. It can be used to support or to refute the occurrence of a crime and also to provide useful information in proving the intent of committing a crime, which is key to prosecution (Casey, 2004). This paper therefore, aims to discuss legal requirements of evidence and then discuss the sufficiency of the Windows event log as source of evidence in digital forensics.

2 Legal requirement for Evidence

The legal requirement for evidence is that it satisfies two tests: admissibility (evidence must be in conformity to certain legal rules) and weight (must be understood and must be convincing enough to the court).

2.1 Admissibility: The general standard for admissibility of evidence is to prove that the evidence is relevant, authentic and reliable It is also required that evidence satisfy the best evidence rule and does not contain hearsay unless if it is classified as an exception to the hearsay prohibition rule before it is admitted as evidence in court (Kenneally, 2004).

2.1.1 Authentic and reliable*:* The requirements for the authentication of evidence to satisfy the court are:

- The evidence was not altered during collection and
- It actually comes from the claimed source – human or machine.
- Supplementary information such as date of record to be used as evidence is accurate. (Casey 2004).

Two steps are involved in authenticating digital evidence. The first step involves the examination of the evidence to determine whether it is what the proponent purports and that it originates from the claimed source. Authenticity of digital evidence can be verified if the person who has collected the evidence testifies that the integrity of the evidence has been maintained and that the evidence originates from the claimed source. The second step of the authentication process involves analysis of the evidence to ascertain its probative value (Casey, 2004). Digital evidence is acceptable in court if a witness who is versed in computer operation can testify that the evidence is authentic and reliable (Kenneally, 2004).

After evidence is authenticated and accepted in court its reliability is evaluated to ascertain its probative value. The evidence must be cogent and understandable (Sommer,1999). Doubts regarding the integrity of evidence reduce the weight of evidence in court Digital evidence is acceptable in court if the party presenting it can prove that the information is reliable and the reliability can be verified by the opposing party in court (Ryan and Shpantzer, 2002).

2.1.2 Satisfy the best evidence rule*:*

Writing **-** The best evidence rule requires that original evidence to be provided before evidence is acceptable in court. Evidence in the form of writing is required to satisfy the best evidence rule. However, because exact and accurate copies of the original evidence can be made, duplicate copies are now acceptable and since computers are capable of producing an accurate copy of the digital evidence, printout of digital evidence are usually acceptable in court.

Hearsay – the rule of hearsay is applicable to all evidence unless it falls within exception to the hearsay prohibition. According to Casey 2004 pp179 "Evidence contained in a document is hearsay if the document is produced to prove that a statement made in court is true". For example, e-mail message may be used to demonstrate that an individual made a statement but it cannot be used to prove the veracity of the content of the e-mail (Casey, 2004).Digital evidence is classified as computer generated or computer stored or hybrid.

Computer generated- this is evidence consisting of output from a computer program e.g., ATM receipt phone records. Courts admit computer generated record providing an expert witness testifies that the computer that generated the record produced an accurate result and was functioning properly (Kenneally, 2004).

Computer Stored- Computer stored evidence are electronic data consisting the writing and statement of an individual e.g. e-mail, business correspondence. Computer stored evidence has more ambiguous standard of authenticity than computer generated. Requirements of some court are that the same standard of authenticating physical document be applied to computer stored – advocates must demonstrate firsthand knowledge of the evidence.

Hybrid- hybrid combines the features of both computer generated and computer stored. Computer generated records are classified under the business record exception to hearsay rule prohibition. Computer generated data are not regarded as hearsay as they do not consist of human statement rather they document an action (Casey, 2004).

2.2 Weight: The weight of evidence is a non-scientific concept. After evidence is accepted in court the next step of the evaluation process is to assess its weight. There isn't any classification of evidence that a court is compelled to accept. The differences between admissibility and weight are unclear especially in scientific evidence. In assessing the weight of evidence a number of features are put into consideration. Based on these features the weight evidence carries is determined.

2.2.1 Authenticity- the evidence is connected to the circumstances and the suspect.

2.2.2 Accuracy- evidence must be convincing and error free; evidence must be acquired using standard accepted procedure by an expert who is able to explain the procedure (Sommer, 1999).

2.2.3 Completeness- evidence must be capable of telling in- its- term the whole event that occurred (Sommer, 1999).

2.2.4 Clear Chain of custody- in assessing the weight of evidence the manner in which evidence is handled right from collection to the time is presented to court put into consideration. All people who handled the evidence and actions performed on the evidence should be documented. The condition of the evidence at the time of collection should be described.

2.2.5 Transparency of forensic procedure- The forensic procedures should be transparent such that a third party can follow the same method and arrive at the same conclusion (Sommer, 1999).

3 Legal standards applied to digital logs

Because digital logs are used as evidence in court, it is therefore, required that the logs satisfy legal standards applied to evidence. As discussed earlier evidence are generally required to conform to certain legal rules before being admitted as evidence. The rules require that evidence is authentic, reliable and relevant. Also required is that evidence does not contain hearsay and that it satisfies the rule of best evidence.

3.1 Authentication and log evidence: It has been discussed earlier that evidence is authentic if originates from the claimed source and that its integrity has not been compromised. The rule applies to log evidence as well. As earlier discussed computer evidence is classified in court as computer-generated, computer stored or hybrid. Based on this classification the court determines how to scrutinize digital log before admittance. There is no over-arching prescription for classifying digital logs therefore; its admissibility is open to case by case decision. For computer generated record, Courts admit computer generated record providing an expert witness testifies that the computer that generated the record produced an accurate result and was functioning properly.

3.2 Log and best evidence rule: as discussed earlier the best evidence rule requires that evidence is original before it is admissible in court. The standard is applied to ensure its credibility. In the case of computer record, printouts or other output that exactly represent that they are regarded as original. Therefore, accurate printout of computer records is accepted as evidence in court. Digital logs satisfy the best evidence rule if the MD5 hashes of the original and the copy matches.

3.3 Digital log and hearsa*y*: The application of the rule of hearsay to digital logs depends on the way a court classifies the log- computer generated, computer stored or hybrid. As described earlier. Computer generated are classified under the business record exception to hearsay prohibition rule (Kenneally, 2004). Computer generated records have been classified as non hearsay because its proponent have been able to demonstrate to the court that the records are merely the product of a computer operating under a set of programme with no human intervention (Casey 2004).

4 Methodology

In order to achieve the objective of this paper, analysing the sufficiency of the Windows event log as evidence in digital forensic investigation, experiments were conducted within a virtual network environment. The virtual network was set up using VMware workstation. Within the virtual network configuration, cyber crime related activities were emulated to determine the sufficiency of the Windows event log in providing evidence of the attack. The cyber crime activity emulated involves password guessing attack with the aid of the Net Essential tools.

Essential Net Tools used to conduct the password guessing attack on the target system (Window Server 2003 domain controller). Net Essential tool contains a variety of network auditing tool, which includes NetBIOS Auditing Tool. NetBIOS Auditing Tool is used to audit a system that offers NetBIOS file sharing service. It also offers password guessing functionality. NAT is a GUI tool with an interface that requires user to supply the starting IP address and the stopping IP address of the target system. NAT attempts to crack the target system by trying a combination of predefined username and password. Figure 4.1 – 4.3 displays result of the attack.

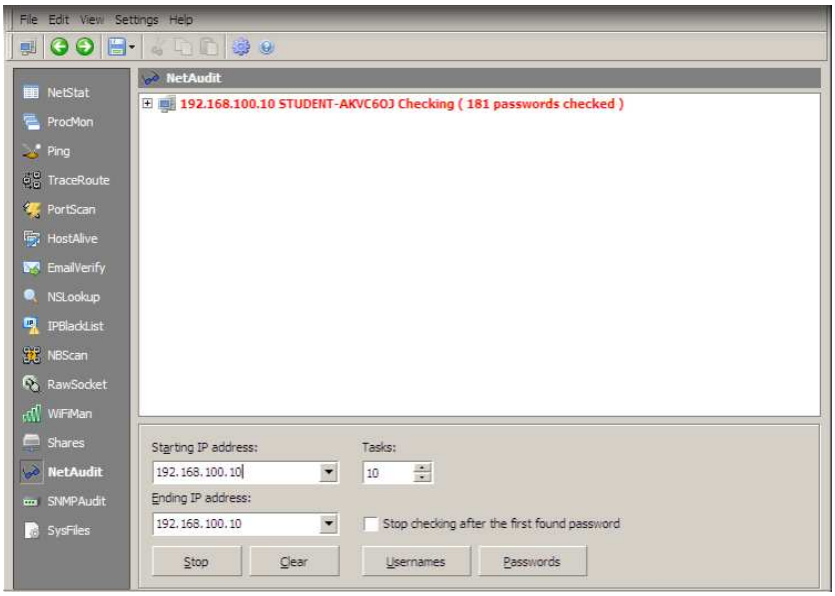


Fig. (4.1): a total of 181 passwords checked on target- Windows Server 2003 domain controller (STUDENT-AKVC6OJ).

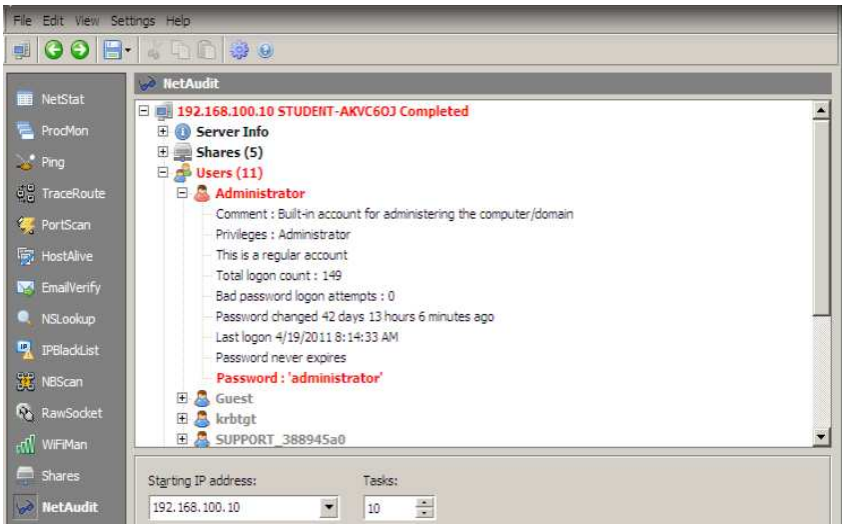


Fig. (4.2): Administrator password found on victim computer.

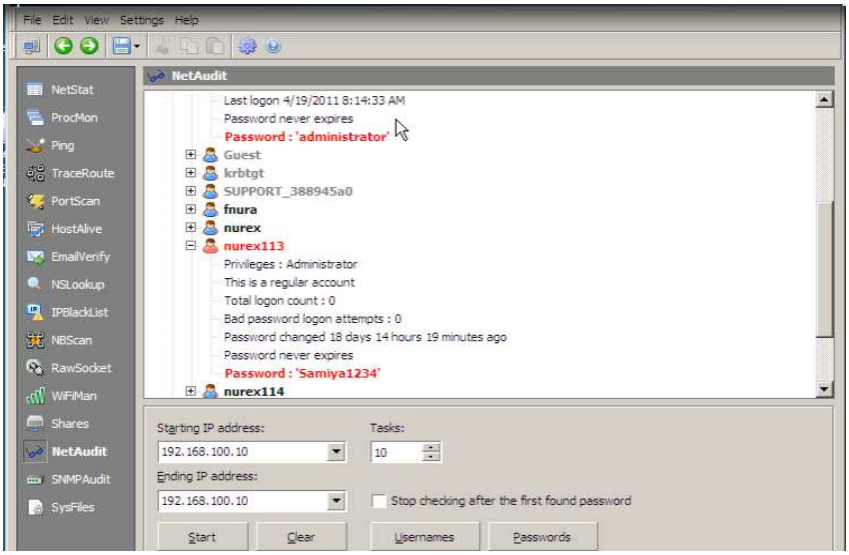


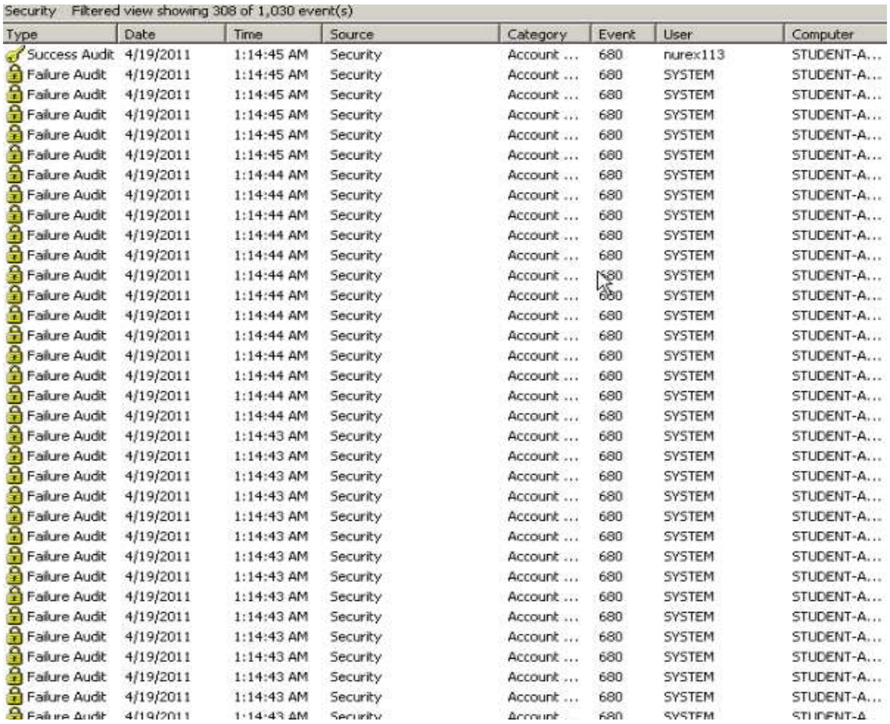
Fig. (4.3): password for user (nurex113) found.

5 Analysis of the Event Logs for Evidence of Attack

The previous section shows that an automated password guessing attack was conducted on a Windows Server 2003 server using NetBIOS Auditing Tool (NAT). The attack involved connecting to an enumerated share (IPC$, C$) on a target (Windows Server 2003) domain controller and then attempting to crack the target with a combination of guessed username and password. During the attack process, a total of 181 passwords were checked (fig 4.1). On completion of the attack five shares including the C$ and ADMIN$ were enumerated on the victim system. A total of eleven users were enumerated (fig 4.3). Passwords for administrator account and a user (nurex113) was discovered on the victim system (fig 4.2 and 4.3).

In this section, the event log is analysed for evidence of activities that occurred during the attack. The attack involved an automated password guessing, therefore, a series of username and password combination will be used by the attacker in attempt to authenticate and logon to the target system. As authentication and logon events are recorded under the account logon and logon events the analysis will be focused on the events generated under the account logon and logon category of the security log in the victim system.

5.1 Examination of the Security Log on the Victim Computer for Evidence of Failed Account Logon Events: As the victim computer is a Window Server 2003 domain controller, both account logon and logon events will be recorded in the security log of the victim computer. The account logon event logs only authentication events (Microsoft, 2011).Because the attack was conducted from a local account and Microsoft uses NTLM to authenticate local accounts; Event ID 680 was filtered in order to search for failed NTLM authentication as shown in figure (5.1). A series of failed account logon event was discovered in the security log of victim system. A large number of failed authentications appearing in the security log of the victim computer is a clear sign that the computer was under an automated password guessing attack. In order to obtain more information on the attack, some of the entries were examined to find any correlation between the events as shown in the figure (5.2).



Security Filtered view showing 308 of 1,030 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Success Audit	4/19/2011	1:14:45 AM	Security	Account ...	680	nurex113	STUDENT-A...
Failure Audit	4/19/2011	1:14:45 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:45 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:45 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:45 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:45 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:44 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:44 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:44 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:44 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:44 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:44 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:44 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:44 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:44 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:44 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:44 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:44 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:44 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account ...	680	SYSTEM	STUDENT-A...
Failure Audit	4/19/2011	1:14:43 AM	Security	Account	680	SYSTEM	STUDENT-A

Fig (5.1): a series of failed authentication in security log of victim system.

Fig (5.2): Event ID 680 recorded when the attacker successfully logon to the victim system

5.2 Examining the Victim System for Evidence of a Successful Authentication (Account Logon): As shown above, the attacker hacked into the passwords of the administrator (Administrator) and the user (nurex113) accounts; subsequently the attacker successfully authenticated to the victim. In Windows Server 2003, Event ID 680 is used to record both failed and successful NTLM authentication. Event ID 680 with success audit was recorded in the security log of the victim system as shown in fig (5.3) and (5.4). The event logs generated in fig (5.3) and (5.4) also provides evidence that the attacker has successfully guessed two passwords from the target system.

Fig. (5.3): Event ID 680 recorded when the attacker successfully guessed and logon with the user account nurex113.

Fig. (5.4): Event ID 680 recorded when the attacker successfully logon to the victim system.

5.3 Examining the Victim system for Evidence of Failed Logon Events: Logon event is generated when a user is attempting to access a resource on a computer. Before a user can logon to a computer the user must be authenticated. If the authentication (account logon) succeeds then the user is granted access (logon) to a system. If, however, the authentication fails the user is denied access to the system. The authentication process and the resulting event generated have been discussed in the previous section. This section discusses the evidence provided by the Windows event log due to failed logon. A large number of failed logon events are also recorded in the security log of the victim system and they are an indication that an unauthorised person is attempting to logon to the target system. After filtering for Event ID 529 in the security log, a large number of failed logon events were revealed. A security log full of failed logon events is a sign that the computer is under an automated password guessing attack as shown in fig. (5.5). However, In order to obtain more information on the failed logon,

some of the entries was viewed and examined as shown in fig (5.6) and (5.7).

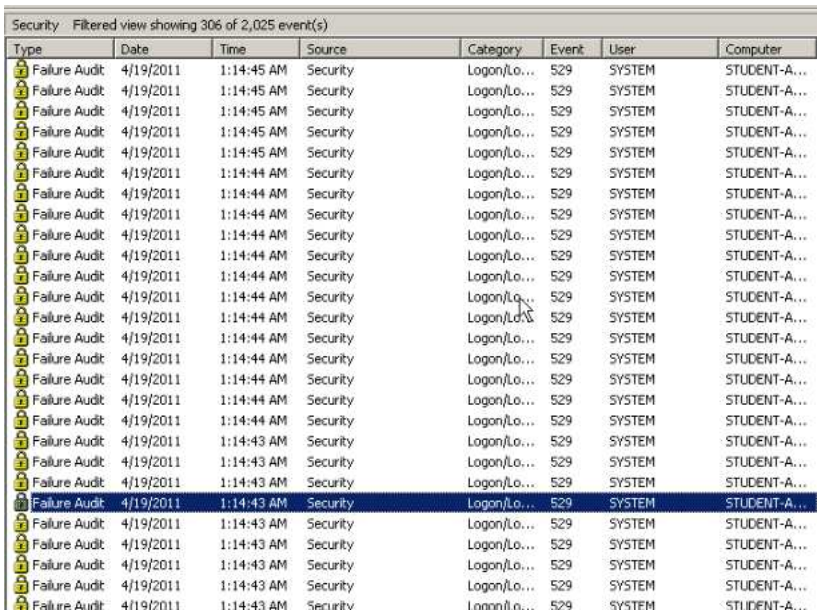


Fig (5.5): a series of failed logon events in security log of victim system.

Fig (5.6): Event ID 529 showing failed logon for user nurex113.

Fig (5.7): The bottom of description field for the same Event ID 529.

5.4 Examining the Victim System for Evidence of Successful Logon Events: As demonstrated above, the attacker has successfully obtained the password for two accounts, the administrator account and the user account (nurex113) and subsequently logon with their credentials. This results in an Event ID 540 to be logged in the victim computer. Event ID 540 indicates that the attacker logged on from a network .Figures (5.8) and (5.9) below shows event generated as a result of a successful logon.

Fig (5.8): Event ID 540 showing successful logon for user account administrator.

Fig (5.9): The bottom of description field for the same Event ID 540.

6 Evaluating the Sufficiency of the Windows Event Log as Evidence

In the previous sections, the security log of the victim system has been examined and analysed for evidence of the cyber crime activities emulated. In this section the evidence obtained are analysed to determine whether they satisfy the legal standard applied to digital logs and evidence in general. It has been mentioned earlier that evidence is required to satisfy two test (admissibility and weight).The admissibility requirement is that evidence satisfy some legal rule such as authenticity, best evidence rule and the hearsay rule. The weight of evidence is assessed based on how the evidence is able to convince the court that the accused is guilty.

6.1 Admissibility of the Windows Event log as Evidence:

- **Authenticity of the Windows Event log:** Evidence provided by the Windows event log is admissible if it can be proven that the evidence is from the claimed source. This can be confirmed by examining the logs generated from the attack. The computer field of each of the events generated shows that the logs were generated by the victim system (STUDENT_AKVC0J).This proves that the logs were authentic and actually originates from the source.
- **The Windows Event log and the hearsay rule:** Log evidence is classified as computer generated. computer generated records are classified as an exception to the hearsay prohibition rule (Kenneally, 2004); therefore, the Windows event log falls under the classification of the hearsay exception prohibition as it is generated by a computer that is operating under a set of program.
- **The Windows Event log and the Best Evidence Rule:** It has been discussed that earlier that log evidence satisfy the best evidence rule and because the Windows event log falls under the category of log evidence, it therefore satisfies the best evidence rule.

6.2 Weight: As discussed earlier, the criteria used in assessing the weight of evidence is that the evidence provides sufficient information needed to convince the court that the crime was perpetrated by the accused (Sommer, 1999). Therefore, in this section the weight of the evidence provided by the Windows Event log after each of the attacks is evaluated.

- **Evaluating the Weight of the Windows Event log for the Password Guessing Attack:** Evidence carries much weight if it can be linked to the circumstances and the suspect and also, if can tell in its own term the whole story of the activities performed by the attacker. (Sommer, 1999). This section will therefore analyse whether the evidence provided by the Windows event log can be linked to the circumstances of the crime and whether it tells the details scenario needed to reconstruct the events that occurred during the incident. After the examination and analysis of the password guessing attack demonstrated above, it was discovered that the Windows event log tells the complete story of the attacker's activities. It provides the following information about the attack:

- From the security log of the victim system a series of failed authentication activities and failed logon activities were discovered and this provides evidence that the victim system was under a password guessing attack.

- Careful examination of the logs further revealed that the attacker has enumerated some user account on the victim system and attempted to logon with their credentials. This evidence was obtained from viewing the entries of failed account logon and logon events.
- It also provided evidence that the attacker successfully cracked the victim system and discovered passwords for 2 users as previously discussed. This evidence was obtained from the successful logon and account logon events (figure 5.3 and 5.8).
- It provided the attacker workstation as WIN2K8 (figure 5.8)
- It provided the IP address of the attacker as 192.168.100.15 as shown in figure (5.9).

In conclusion, the analysis of the Windows event log proves that it provides all the evidence needed to reconstruct the activities performed during the password guessing attack and also to link the attack to the actual perpetrator. Hence, it will carry much weight in court.

7 Conclusion

This paper has investigated the question of sufficiency of windows event logs in serving as digital forensics evidence that could be accepted in the court of law. it has been discussed that evidence must satisfy two the admissibility and weight test The admissibility test requires that evidence conform to certain legal standard such as authenticity, reliability and that the evidence most not contain hearsay. After evidence is admitted in court its weight is accessed to determine its probative value. In evaluating the weight evidence, what is most considered is that the evidence be able to convince the court that the offence was perpetrated by the accused. cyber crime activities were emulated on a Windows Server 2003. The cyber crime activities emulated involved password guessing attack and exploitation of the Windows network service.

References:

1. Abdullah, M.T., Mahmood, R., Ghani, A.A.A., Abdullah, M.Z. and Sultan A. M. S. (2008) *Advances in computer forensics*,8 (2),pp 215-219
2. Casey, E. (2004) *Digital evidence and computer crime: forensic science computer and internet*, 2nd edn. London: Academic press.
3. Dashora, K., Tomar, D.S. and Rana, J.L. (2010) *A practical approach to evidence gathering in Windows environment*, 5 (8), pp.21-27.
4. Kenneally, E.E. (2004) *Digital logs-proof matters*, 1(2), pp.94-101.
5. Ryan, D. J. and Shpantzer (2002) *Legal aspect of digital forensic* [Online]. Available at: http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf (Accessed: 25 March 2011).
6. Sommer, P. (1999) *Intrusion detection as evidence*, 31(23-24), pp. 2477-2487.
7. Schuster, A. (2007) *Introducing the Microsoft vista event log file format*, 4(1), pp. 65- 72.
8. Stallings, W. and Brown, L., (2008) *Computer security*: *principle and practice*. NJ: Pearson Education Inc
9. Steel, C. (2006) *Windows forensic: The field guide for corporate computer Investigations*: John Wiley and Sons.
10. StrathclydeForensics, (n.d) *Windows forensics*. Available at: http://www.strathclydeforensics.co.uk/windows_forensics.htm (Accessed: 12 March 2011)
11. Wang, S.J. (2006) *Measures of retaining digital evidence to prosecute computer-based cyber-crime*, 29(2), pp.216-223.
12. Wang, G., Cannady, J., and Rosenbluth, J. (2005) *Foundation of computer forensics: A technology for the fight against cyber-crime*, 21(2), pp.119-127.