International Journal of Computer Applications Technology and Research
Volume 4– Issue 6, 425 - 434, 2015, ISSN:- 2319–8656

Securing an Information Systems from Threats: A Critical Review

Grace L. Samson
Department of Computer Science
University of Abuja
Gwagwalada–Abuja, Nigeria

Mistura M. Usman
Department of Computer Science
University of Abuja
Gwagwalada-Abuja, Nigeria

Abstract: The technology behind information systems in today's world has been embedded in nearly every aspect of our lives. Thus, the idea of securing our information systems and/or computer networks has become very paramount. Owing to the significance of computer networks in transporting the information and knowledge generated by the increased diversity and sophistication of computational machinery, it would be very imperative to engage the services of network security professionals to manage the resources that are passed through the various terminals (end points) of the these network, so as to achieve a maximum reliability of the information passed, making sure that this is achieved without creating a discrepancy between the security and usability of such network. This paper examines the various techniques involved in securely maintaining the safe states of an active computer network, its resources and the information it carries. We examined techniques of compromising an information system by breaking into the system without authorised access (Hacking), we also looked at the various phases of digital analysis of an already compromised system, and then we investigated the tools and techniques for digitally analysing a compromised system in other to bring it back to a safe state.

Keywords: Computer Security, Hacking, Digital Analysis, Computer Networks, Risk and Vulnerability

1. INTRODUCTION

Computer Networks according to [1] satisfy a broad range of purposes and meet various requirements which include (a) Provide the sharing of resources such as information or processors, (b) provide inter-process communication among users and processors, (c) provide distribution of processing functions, (d) provide centralised control for a geographically distributed system, (e) provide centralised management and allocation of network resources etc. The most important characteristic of a computer network as identified by [2] is its generality. Computer networks are built primarily from general-purpose programmable hardware, and they are not optimized for a particular application like making phone calls or delivering television signals. Instead, they are able to carry many different types of data, and they support a wide and ever-growing range of applications. A computer network therefore means an interconnected collection of autonomous computers [1]. Owing to this significance of computer networks in transporting the information and knowledge generated by the increased diversity and sophistication of computational machinery [3], it would be very imperative to engage the services of network security professionals to manage the resources that are passed through the various terminals (end points) of these networks, so as to achieve a maximum reliability of the information passed over these networks making sure that this is achieved without creating a discrepancy between the security and usability of such network – since these two are the main concerns of any network owners. Consequently, the issue of managing a computer network should include finding a balance between security and usability of the network so as to achieve the purpose, confidentiality, authenticity, accountability, availability and of course integrity of that network

1.1 Computer Security

[4] Identified three main factors that could be encountered in managing a computer network. According to him these include *assets*, *threats*, *vulnerability* and *risk*, where;

Risk = assets + threats + vulnerability [4]

However, he also acknowledged the fact that computer security has to do with the protection of assets from threats and vulnerability in other to reduce the amount of risk the system may face.

[5], in his own view defined the security of an information system as the state of being *free* from danger and being unexposed to damage from accidents or attacks of any form. He also added that computer security is a process of achieving a state that is optimally desirable for an information system; stating clearly that the main goal of an information system security is to optimize the performance of the system with respect to the measure of risk to which the system is exposed to. [6] describes Computer security in this form and he states; "If a system always stays in states that are allowed, and users can only perform actions that are allowed, the system is *secure*. But if the system can enter a disallowed state, or if a user can successfully execute a disallowed action, the system is *non-secure"* [6].

The technology behind information systems in today's world according to [7] has been embedded in nearly every aspect of our lives. Thus, the idea of securing our information systems and/or computer networks has become very paramount. According to them, the major reason for securing information systems is to attain the five main tenets of a secured system. Specifically, *network security* is the ability of a computer network to provide one of the services expected of an information system [8]; the first four *confidentiality*, *integrity*, *authentication* and n*onrepudiation* has to do with the *message being exchanged over the network* and the other one has to do with *authentication of users* (see figure 1).

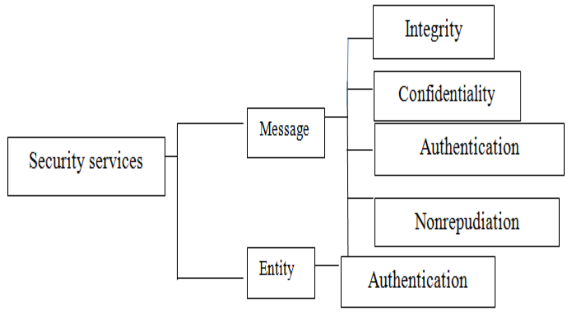


Figure 1: Network Security Services

1.2 Importance of computer security

According to [9], computer networks are a group of devices that represent a shared resource used by many applications that symbolises different kinds of interest thus, unless security measures are taken, any network conversation or distributed application may be interrupted by a saboteur. Thus the importance of computer security according to [10] is to be able to achieve a balance between *usability* and *security*; a network/information system owner should therefore be able to define its organizational information system objectives to cover the three goals of a secured information system (which includes Confidentiality, Integrity and Availability - CIA).

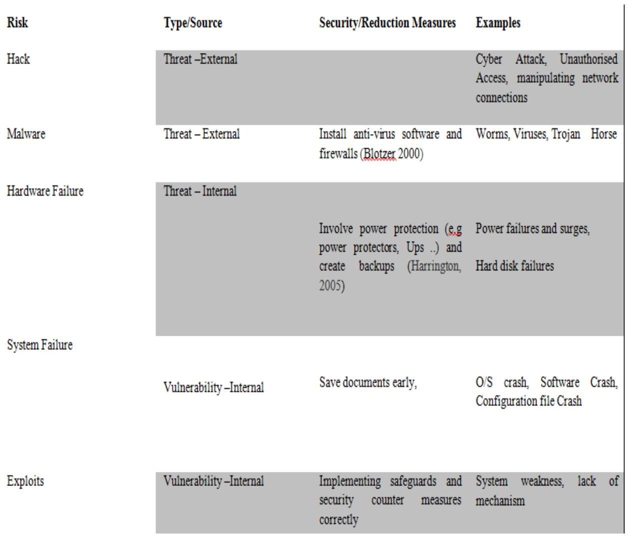
1.3 Security Mechanisms

Computer security measures aims to prevent security violations; as such, researchers have developed technologies that could be counted on to prevent computers from leaking sensitive data, and the need for competing interests to share a common set of computing resources lies at the heart of many computer security requirements [11]. The answer to the question of how to ensure that a computer network/information system is secured lies in the nature or form of attack to which the system(s) is exposed to. The table below summarises these forms of risk and some of the security measures that can be taken to avert or minimize them.

1.4 Security Mechanisms

Computer security measures aims to prevent security violations; as such, researchers have developed technologies that could be counted on to prevent computers from leaking sensitive data, and the need for competing interests to share a common set of computing resources lies at the heart of many computer security requirements [11]. The answer to the question of how to ensure that a computer network/information system is secured lies in the nature or form of attack to which the system(s) is exposed to. The table below summarises these forms of risk and some of the security measures that can be taken to avert or minimize them.

Table **1**: Computer/ information System Risk Security Measures



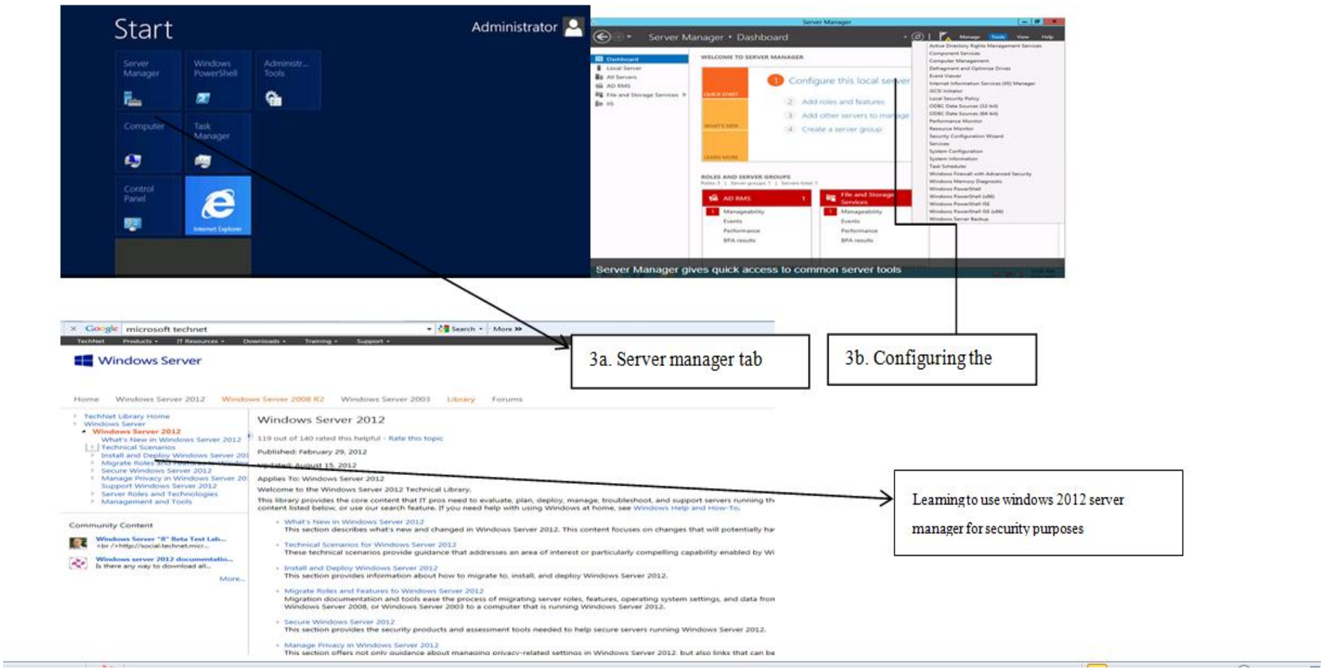
Risk	Type/Source	Security/Reduction Measures	Examples
Hack	Threat –External		Cyber Attack, Unauthorised Access, manipulating network connections
Malware	Threat – External	Install anti-virus software and firewalls (Blotzer 2000)	Worms, Viruses, Trojan Horse
Hardware Failure	Threat – Internal	Involve power protection (e.g power protectors, Ups ..) and create backups (Harrington, 2005)	Power failures and surges, Hard disk failures
System Failure	Vulnerability –Internal	Save documents early,	O/S crash, Software Crash, Configuration file Crash
Exploits	Vulnerability –Internal	Implementing safeguards and security counter measures correctly	System weakness, lack of mechanism

In addition, securing an information system would also mean building a secured system or a secured organizational network. [12] has identified some basic steps necessary to achieve this aim; these include the fact that every network administrator/owner should:

- Always evaluate session Risks and Threats
- Beware of common misconception (e.g ignoring a session being too small a target to malicious act)
- Always provide security training for IT staff
- Beware of external attacks against a session (e.g avoid threats from portable handheld external storage devices; like USB flash derive that could easily transfer organizations data out to a hoodlum and also avoid threats from storing data online where users can log in and easily transfer files or the online storage may be short-lived)
- Security features of operating systems should be identified and utilised (e.g using the windows server manger as shown in figure 2a/b below and in other to learn how to use this feature, see figure 2c)
- Other things the system administrator can do is to always monitor the systems
- A third party always auditing the organisation's security and then
- Never forget patching your network facilities

- Remember little thing like;
  - Making sure to change default system password
  - Use a password that is not trivial
  - Always close every unnecessary ports

In general, in other to protect a company's network from hoodlums, companies' employ the services of *ethical hackers* to do exactly what the hoodlums will want to do illegally so as to find loop holes in their security system [13].



Server Manager gives quick access to common server tools

Windows Server 2012

119 out of 140 rated this helpful - Rate this topic

Published: February 29, 2012

Updated: August 15, 2012

Applies To: Windows Server 2012

Welcome to the Windows Server 2012 Technical Library.

This library provides the core content that IT pros need to evaluate, plan, deploy, manage, troubleshoot, and support servers running th content listed below, or use our search feature. If you need help with using Windows at home, see Windows Help and How-To.

- What's New in Windows Server 2012
  This section describes what's new and changed in Windows Server 2012. This content focuses on changes that will potentially ha
- Technical Scenarios for Windows Server 2012
  These technical scenarios provide guidance that addresses an area of interest or particularly compelling capability enabled by Wi
- Install and Deploy Windows Server 2012
  This section provides information about how to migrate to, install, and deploy Windows Server 2012.
- Migrate Roles and Features to Windows Server 2012
  Migration documentation and tools ease the process of migrating server roles, features, operating system settings, and data fron Windows Server 2008, or Windows Server 2003 to a computer that is running Windows Server 2012.
- Secure Windows Server 2012
  This section provides the security products and assessment tools needed to help secure servers running Windows Server 2012.
- Manage Privacy in Windows Server 2012
  This section offers not only guidance about managing privacy-related settings in Windows Server 2012, but also links that can be

Windows Server "8" Beta Test Lab...
<br />http://social.technet.micr...

Windows server 2012 documentatio...
Is there any way to download all...

Figure 2c: how to use windows security facilities

2. HACKING

The essence of this section is to bring to our attention the major security issues that are worth mentioning in a discussion of network security of which the most obvious of these is computer network *hacking*.

2.0 What is hacking?

Hacking means getting access to and secretly looking at or changing information on a computer network resource or its information without an authorised permission. In other words it involves finding an unintended or overlooked use of an information system in an innovative way in other to use the outcome to solve a given problem [14]. Hacking tools are basically codes which a hacker writes when he wants to automate a task. [15] has identified three (3) major types of these codes as we have shown below.

Nmap,

Nessus

Netcat.

2.1 The hacking process:

Hacking or cracking a network according to [16] would usually involve the process as described by the diagram below

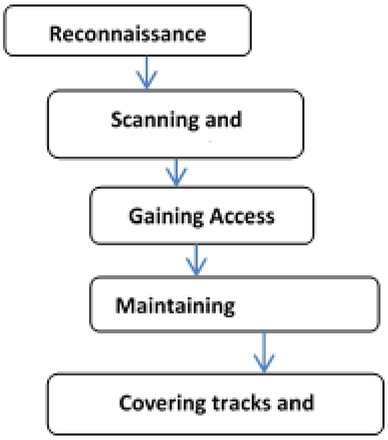
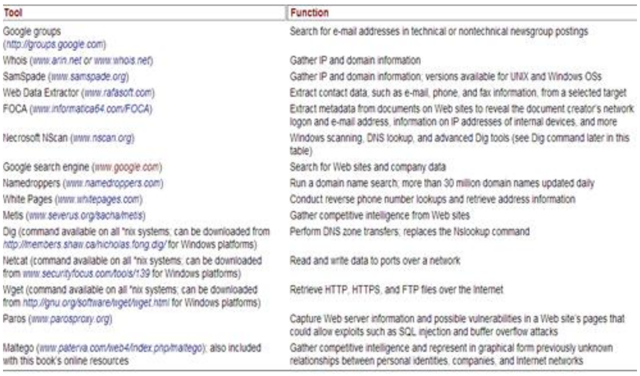


Figure 3: five phases of hacking

2.2 Performing reconnaissance – organization's information system/network exploration

The first step a successful hacker must take is information gathering. This is a way of successfully executing an attack against an organization's information system/network by gathering as much intelligence about the organization as possible. According to [17], some of the methods that one could adopt include: (a) dumpster driving (b) search engine querying (c) public database querying (d) social networking e.t.c

Table 2: detailed tools and information gathered during reconnaissance [13]

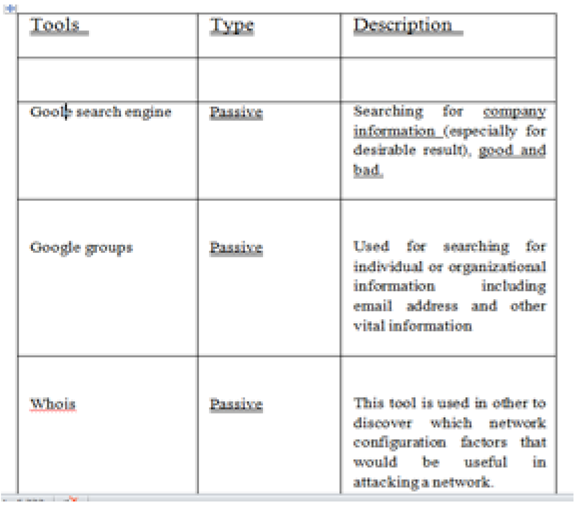


Tool	Function
Google groups (http://groups.google.com)	Search for e-mail addresses in technical or nontechnical newsgroup postings
Whois (www.arin.net or www.whois.net)	Gather IP and domain information
SamSpade (www.samspade.org)	Gather IP and domain information; versions available for UNIX and Windows OSs
Web Data Extractor (www.rafasoft.com)	Extract contact data, such as e-mail, phone, and fax information, from a selected target
FOCA (www.informatica64.com/FOCA)	Extract metadata from documents on Web sites to reveal the document creator's network logon and e-mail address, information on IP addresses of internal devices, and more
Necrosoft NScan (www.nscan.org)	Windows scanning, DNS lookup, and advanced Dig tools (see Dig command later in this table)
Google search engine (www.google.com)	Search for Web sites and company data
Namedroppers (www.namedroppers.com)	Run a domain name search; more than 30 million domain names updated daily
White Pages (www.whitepages.com)	Conduct reverse phone number lookups and retrieve address information
Metis (www.severus.org/sacha/metis)	Gather competitive intelligence from Web sites
Dig (command available on all *nix systems; can be downloaded from http://members.shaw.ca/nicholas.fong/dig/ for Windows platforms)	Perform DNS zone transfers; replaces the Nslookup command
Netcat (command available on all *nix systems; can be downloaded from www.securityfocus.com/tools/139 for Windows platforms)	Read and write data to ports over a network
Wget (command available on all *nix systems; can be downloaded from http://gnu.org/software/wget/wget.html for Windows platforms)	Retrieve HTTP, HTTPS, and FTP files over the Internet
Paros (www.parosproxy.org)	Capture Web server information and possible vulnerabilities in a Web site's pages that could allow exploits such as SQL injection and buffer overflow attacks
Maltego (www.paterva.com/web4/index.php/maltego); also included with this book's online resources	Gather competitive intelligence and represent in graphical form previously unknown relationships between personal identities, companies, and Internet networks

Like any successful hacker, you have to know what you are looking for and the best place to find it is from Company or institutional sites.

2.2.1 *Tools for performing reconnaissance and information gained*

Table 3: brief summary of passive reconnaissance tools



Tools	Type	Description
Goole search engine	Passive	Searching for company information (especially for desirable result), good and bad.
Google groups	Passive	Used for searching for individual or organizational information including email address and other vital information
Whois	Passive	This tool is used in other to discover which network configuration factors that would be useful in attacking a network.

2.3 Scanning/Enumerating – organization's information system/network exploration

Active reconnaissance *(network scanning/enumeration)* involves probing the targeted network or a specific host, in other to detect vulnerabilities. Many attackers will avoid active scanning, because it will often leave traces in the target system's logs, making their activities easier to trace. Active scanning include *port scanning to find open ports*, *testing web applications for weak passwords or insecure code*, or *sending web links to user's s*hopping that they will visit a web site that will log their IP address and information that might identify potential attack vectors [18].

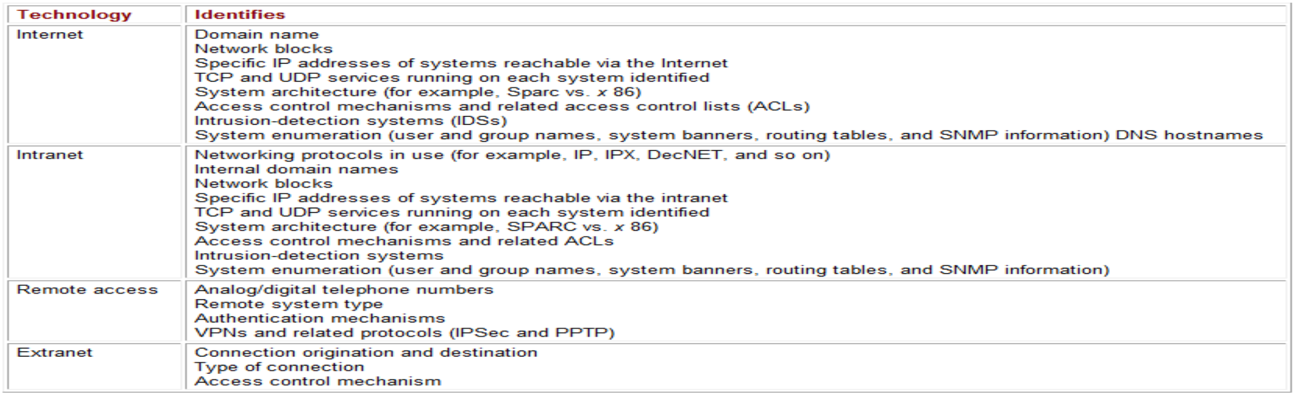
Similarly [19] acknowledged that network scanning can help the attacker to find IP address range, show live addresses, device manufacturer, MAC address, any available user, and DNS name. It can also be used to identify shared folders, HTTP, HTTPS and FTP. Network scanning can easily be achieved through the internet by using methods like ping tool discovery, port scan and ping sweep. Scanning is used, for recognizing active machines and finding open ports and access points. It is important to note according to [20] that Ports 0 to 1023 are well-known ports used for specific protocols and port 80 is the well-known port for HTTP. Thus If a port scan discovers port 80 open, the attacker knows that HTTP (which is most likely a web server) is very likely running on the system. A further attack after finding *open ports, live systems and operating systems* is *enumeration*. [18] describes network enumeration as a process of identifying domain names and their associated networks. At this hacking stage according to [13], the hacker tries to identify resources that are shared on the network (by using specific OS tools), discover user accounts login (probably by guessing of passwords after determining a username) and attempt to retrieve information and gain access to servers by using company employees' logon accounts already discovered.

- **Tools for scanning an organization's network and information gained**

Hacking tools are basically codes which a hacker writes when he wants to automate a task. In general, some major tools for scanning according to [16] include;

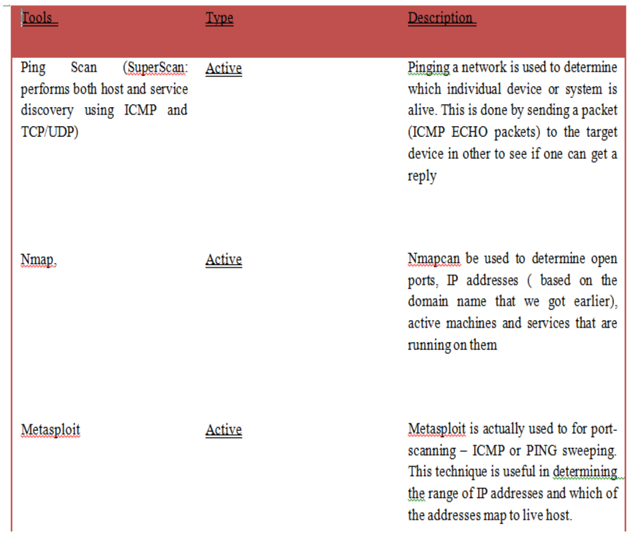
- Internet control message protocols (ICMP) scanners
- Scanners
- Diallers
- Ping sweep
- Mappers e.t.c

Table 4 : detailed identifiable information during hacking and what the hacker can get [21]



Technology	Identifies
Internet	Domain name Network blocks Specific IP addresses of systems reachable via the Internet TCP and UDP services running on each system identified System architecture (for example, Sparc vs. x 86) Access control mechanisms and related access control lists (ACLs) Intrusion-detection systems (IDSs) System enumeration (user and group names, system banners, routing tables, and SNMP information) DNS hostnames
Intranet	Networking protocols in use (for example, IP, IPX, DecNET, and so on) Internal domain names Network blocks Specific IP addresses of systems reachable via the intranet TCP and UDP services running on each system identified System architecture (for example, SPARC vs. x 86) Access control mechanisms and related ACLs Intrusion-detection systems System enumeration (user and group names, system banners, routing tables, and SNMP information)
Remote access	Analog/digital telephone numbers Remote system type Authentication mechanisms VPNs and related protocols (IPSec and PPTP)
Extranet	Connection origination and destination Type of connection Access control mechanism

Table 5: network scanning tools and information obtained



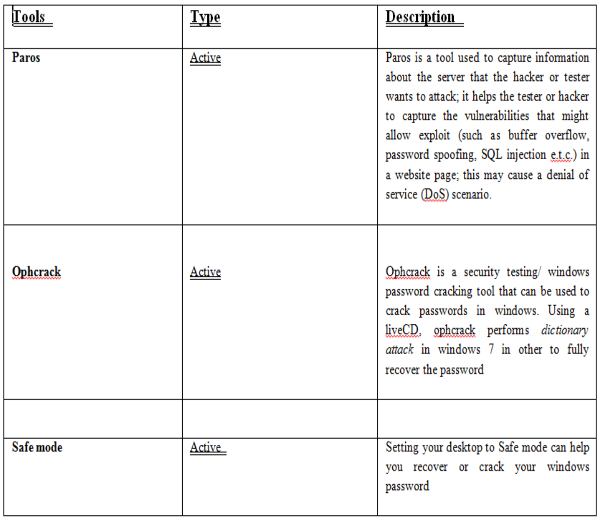
Tools	Type	Description
Ping Scan (SuperScan: performs both host and service discovery using ICMP and TCP/UDP)	Active	Pinging a network is used to determine which individual device or system is alive. This is done by sending a packet (ICMP ECHO packets) to the target device in other to see if one can get a reply
Nmap,	Active	Nmapcan be used to determine open ports, IP addresses (based on the domain name that we got earlier), active machines and services that are running on them
Metasploit	Active	Metasploit is actually used to for port-scanning – ICMP or PING sweeping. This technique is useful in determining the range of IP addresses and which of the addresses map to live host.

1.1.1 Gaining Access

This is the stage when an attacker actually gains full control over a targeted machine [22]. In a more general note, this actually involves *finding vulnerability* in a network server, which according to [23] can be achieved by misusing an application server or by disassembling network security in other to gain maximum access. Some of the vulnerability that could be discovered includes: Misconfigured (or poisoned) web and mail servers running services such as FTP (could be exposed to attack such as *buffer overflow* which gives the hacker a full system *root privilege to the internal host* – [24], *denial of service* or even *session hijacking).*Some of the connection method that the hacker or tester may use for exploit may be; a local access to a pc, the internet, local area network (LAN). According to [25], gaining access is where the damage is usually done and its mostly carried out by using methods like spoofing, smurf attacks e.t.c.

2.4.1 Tools for Gaining access and information gained

Table 6: gaining access tools and information obtained



Tools	Type	Description
Paros	Active	Paros is a tool used to capture information about the server that the hacker or tester wants to attack; it helps the tester or hacker to capture the vulnerabilities that might allow exploit (such as buffer overflow, password spoofing, SQL injection e.t.c.) in a website page; this may cause a denial of service (DoS) scenario.
Ophcrack	Active	Ophcrack is a security testing/ windows password cracking tool that can be used to crack passwords in windows. Using a liveCD, ophcrack performs *dictionary attack* in windows 7 in other to fully recover the password
Safe mode	Active	Setting your desktop to Safe mode can help you recover or crack your windows password

2.5Escalating Privileges

After gaining access, the hacker would want to maintain that access and then apply it to future exploitation, attacks or testing. Occasionally, hackers toughen the systems and make them inaccessible from other hackers or security tester by securing their exclusive access with backdoors, rootkits, and Trojans, this can help to launch additional attacks. [16] describes escalation of privilege as "the act of leveraging a bug or vulnerability operating system or an application" in other to have full control of the system. He also added in [16] that this stage entails adding more rights or permissions to a user account, in other words turning a regular user account into an administrator account. At this stage, the hacker begins to execute applications such as copying of files or even damaging system information. [25] added that the major attacks in this phase include: operating systems attack, application level attack, shrink-wrap code attack and misconfiguration attack. Some of the tools for escalating privilege according to [26] include;

Key-stroke logger -: this tool helps the attacker to exploit the OS by stealing an administrator access, manipulating scheduled task, social engineering, remote control program e.t.c.

Safe Mode –: the hacker boots the system in safe mode and then changes his access level to that of an administrator, there by gaining access to different layers in the system.

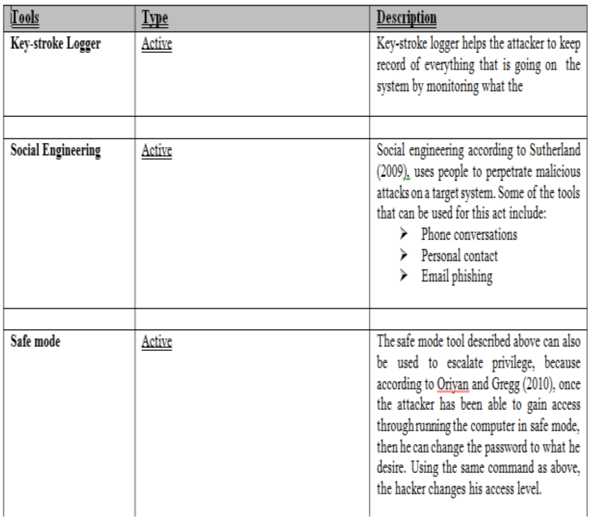
Social Engineering-: in other to gain administrative domain privilege sometimes according to [27], the computer may not be touched; in this case social engineering may be the common path. This tool can be used by manipulating people into \aperforming an action or providing information through means such as using phones, phishing emails or contacting the person.

In addition, according to [27], some of the techniques for escalating privileges in windows include:

- Clearing text passwords stored in files
- Clearing text passwords stored in Registry
- Writing access to the system 32 directory
- Writing access to the all users start up folder
- Windows services running as a system
- Installing a user defined service
- Weak application configuration

- ***Tools for escalating privileges after gaining access***

Table 7: escalating privileges tools and information obtained



Tools	Type	Description
Key-stroke Logger	Active	Key-stroke logger helps the attacker to keep record of everything that is going on the system by monitoring what the
Social Engineering	Active	Social engineering according to Sutherland (2009), uses people to perpetrate malicious attacks on a target system. Some of the tools that can be used for this act include: ➢ Phone conversations ➢ Personal contact ➢ Email phishing
Safe mode	Active	The safe mode tool described above can also be used to escalate privilege, because according to Oriyan and Gregg (2010), once the attacker has been able to gain access through running the computer in safe mode, then he can change the password to what he desire. Using the same command as above, the hacker changes his access level.

Finally, decode the content of the document using the logger program and you get back the unsaved file. The key stroke logger helps the hacker in the escalating privilege phase to be able to have full control of the system while he monitors all transactions going on, on the keyboard.

2.6 Maintaining Access / Placing Backdoors and Covering Tracks

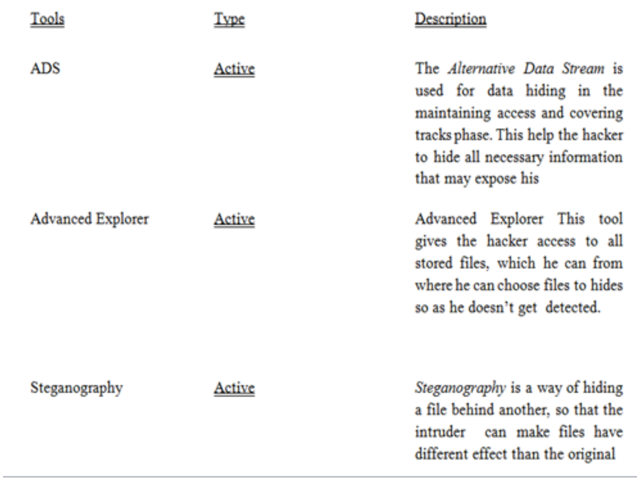
This final hacking stage or the penetrating/hacking process as identified by [22] has to do with avoiding detection (by covering tracks and placing backdoors). This can be done by trying to avoid evasion detection by antivirus software. In other to avoid the embarrassment of being caught, the *hacker* creates unique payloads (which will not match any available signatures) to run on the antivirus software. In other for the hacker to maintain full access and control, they close up every vulnerability so as to stop other attackers or security personnel from detecting their act on the system. They continue to own the system, remove all hacking evidence, or even avoid illegal action. Some of the actions the hacker performs at this stage include; *tunnelling, altering log files* and *steganography*. In their own view, covering tracks needs to be a systematic process in which any evidence of attack (including –logons, log files, error messages …) need to be removed [28].

Some of the things the hacker can do at this phase according to [28] include:

- Disabling auditing
- Data hiding (using ADS – Alternate Data Stream)
- Trojan installation (according to [25] – by executing a script in Trojan rootkit, a variety of critical files are replaced with new versions, hiding the attacker in seconds).

Tools for maintaining access and covering tracks

Table 8 Tools for maintaining access and covering tracks



Tools	Type	Description
ADS	Active	The *Alternative Data Stream* is used for data hiding in the maintaining access and covering tracks phase. This help the hacker to hide all necessary information that may expose his
Advanced Explorer	Active	Advanced Explorer This tool gives the hacker access to all stored files, which he can from where he can choose files to hides so as he doesn't get detected.
Steganography	Active	*Steganography* is a way of hiding a file behind another, so that the intruder can make files have different effect than the original

3 ANALYSING A COMPROMISED SYSTEM

3.1 Introduction:

According to [29], after any of these crimes listed above or incident that involves a computer occurs, a specialist trained in computer forensics examines the computer to find clues about what happened. In most cases, this specialist may work with law enforcement or with a corporate incident response team. Although the rules governing each activity can be dramatically different depending on who your client is, the approach to the investigation remains roughly the same. [30] added that due to the globalisation and the pervasive presence of the Internet these days companies are geographically distributed creating a great business and organisational opportunity. As such, organizational hardware and software related resources such as system administrators, needs expensive management and configuration software available in other to build a timely updated hardware and software changes across the organizational network (whenever there is a reason to make such changes across the network) otherwise organizational system resources may experience an increase in security vulnerability. If this happens without a countermeasure, then there will be a need for digital analysis/ investigation of that compromised system.

Digital analysis is a computer investigation of a compromised system (including - computers, electronics and digital equipment), which involves finding the evidence which will be accepted in the Court of Law and only the investigation which ends with the court admissible evidence is a successful investigation [31]. This type of analysis is a much more involved process where the investigator must trace user activity and cannot provide a simple yes or no answer.

3.2 Phases of digital analysis

This investigation takes the form of five stages according [31] namely;

- Preparing for an incident
- Collection of evidence,
- Preservation of evidence,
- Filtering the evidence,

- Presentation of evidence

3.3 Tools and techniques to digital analysis (Collection and Preservation of evidence)

Some of the tools used for digital analysis as classified by [29] include:

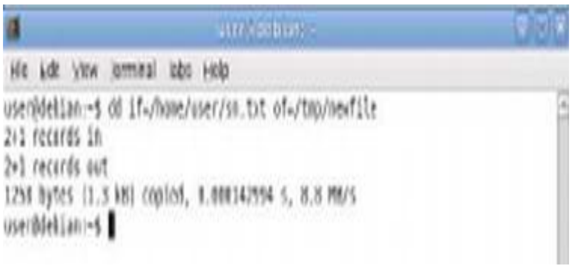
Digital imaging and validation tools – these are tools (depending on OS, functionality and the file system that the tool support) used to make sure media is preserved before any further steps are taken. Preserving the media is necessary to provide assurance the evidence acquired is valid.

Some tools include

- ***dd***

dd is u*sed* in Linux machine for capturing data image using the command

```
dd if=/home/user/sn.txt of=/tmp/newfi
```

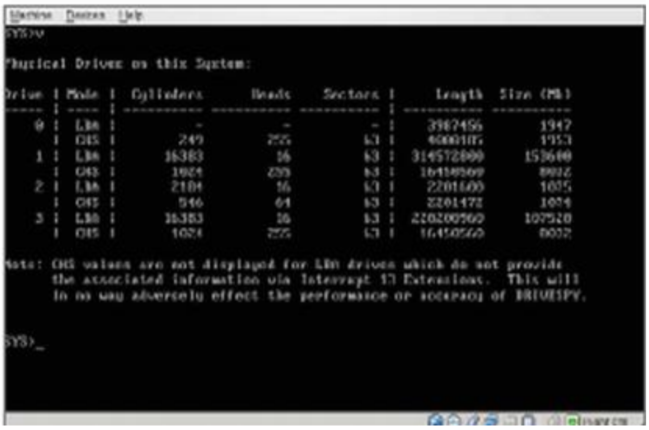


```
user@debian:~$ dd if=/home/user/sn.txt of=/tmp/newfile
2+1 records in
2+1 records out
1258 bytes (1.3 kB) copied, 0.00014294 s, 8.8 MB/s
user@debian:~$ ▌
```

Figure 4: using dd for digital analysis

- ***DriveSpy***

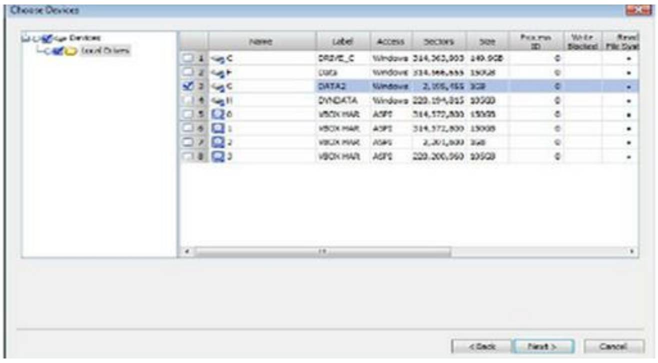
DriveSpy is a DOS based image capturing system of a compromised system. ***DriveSpy*** provides a lot of functions for copying and examining a drive's content



```
SYS>V

Physical Drives on this System:

Drive | Mode |  Cylinders      Heads    Sectors |    Length  Size (MB)
----- | ---- | ---------- ---------- ---------- | ---------- ----------
    0 | LBA  |          -          -          - |    3987456       1947
      | CHS  |        249        255         63 |    4000185       1953
    1 | LBA  |      16383         16         63 |  314572800     153600
      | CHS  |       1024        255         63 |   16450560       8032
    2 | LBA  |       2184         16         63 |    2201600       1075
      | CHS  |        546         64         63 |    2201472       1074
    3 | LBA  |      16383         16         63 |  220200960     107520
      | CHS  |       1024        255         63 |   16450560       8032

Note: CHS values are not displayed for LBA drives which do not provide
      the associated information via Interrupt 13 Extensions.  This will
      in no way adversely effect the performance or accuracy of DRIVESPY.

SYS>_
```

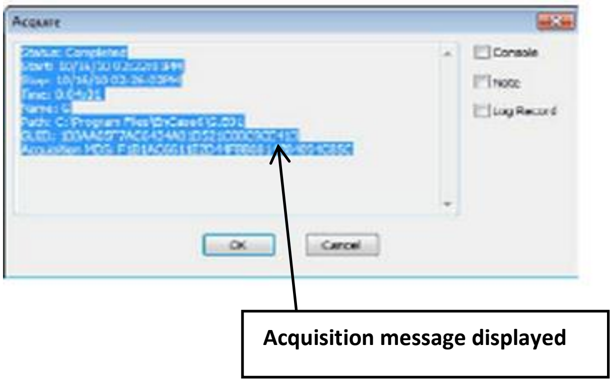
Figure 5: using DriveSpy for digital analysis

- ***Encase*** – this tool produces frameworks for managing a complete case in the analysis of a compromised system.it also include a drive duplicator (known as drive manager) which creates an exact image of the drive and then validates the image automatically see figure below.



		Name	Label	Access	Sectors	Size	Forensic ID	Write Blocked	Read File Sys
□	1	C	DRIVE_C	Windows	314,363,903	149.9GB	0		•
□	2	F	Data	Windows	314,568,[illegible]	150GB	0		•
☑	3	G	DATA2	Windows	2,[illegible]	1GB	0		•
□	4	H	DYNDATA	Windows	220,194,815	105GB	0		•
□	5	0	VBOX HAR	ASPI	314,572,800	150GB	0		•
□	6	1	VBOX HAR	ASPI	314,572,800	150GB	0		•
□	7	2	VBOX HAR	ASPI	2,201,600	1GB	0		•
□	8	3	VBOX HAR	ASPI	220,200,960	105GB	0		•

Figure 6a: using Encase for digital analysis



Status: Completed
Start: 10/16/10 02:22:[illegible] PM
Stop: 10/16/10 02:26:[illegible] PM
Time: 0:04:[illegible]
Name: C
Path: C:\Program Files\EnCase6\C.E01
GUID: [illegible]
Acquisition MD5: [illegible]

Acquisition message displayed

Figure 6b: using Encase for digital analysis

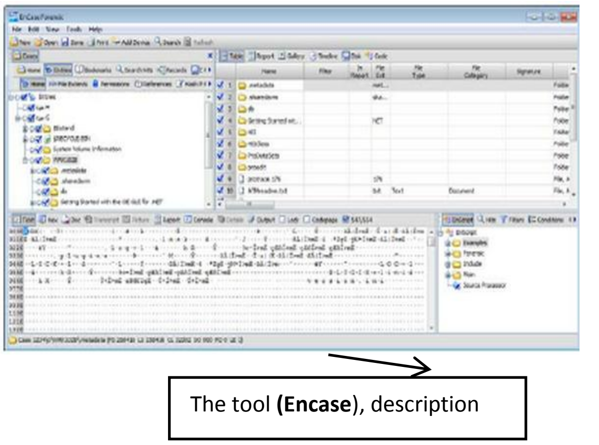
3.4 Forensic tools (Filtering the evidence)

These are the tools used for analysis (depending on you specific investigative need) after the investigator might have made a verified copy of the original media. Your choice of tool will depend on

i. The operating system
ii. The user interface preference
iii. Budget
iv. Functionalities/capabilities

- ***Some of these tools include:***

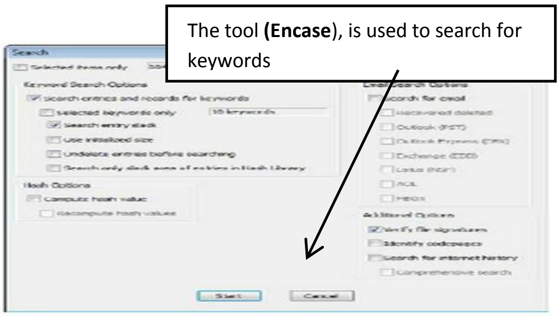
Encase – Encase can also be used for the analysis of the system after a copy of the system has been made as described above. Encase is also useful in terms of viewing the IP addresses.



The tool (**Encase**), description

Figure 7a: using Encase or digital analysis (Filtering the evidence)

.


The tool **(Encase**), is used to search for keywords

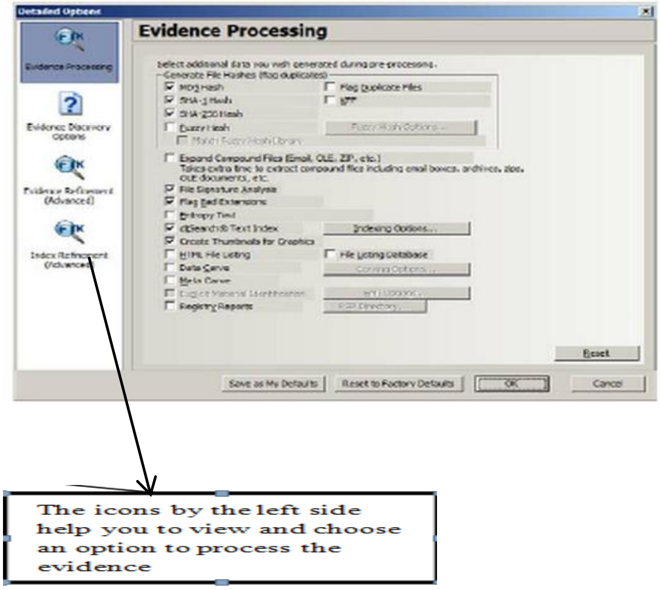
Search

- □ Selected items only
- Keyword Search Options
- ☑ Search entries and records for keywords
- □ selected keywords only — 10 keywords
- ☑ Search entry slack
- □ Use initialized size
- □ Undelete entries before searching
- □ Search only slack area of entries in Hash Library
- Hash Options
- □ Compute hash value
- □ Recompute hash values
- Email Search Options
- □ Search for email
- □ Recovered deleted
- □ Outlook (PST)
- □ Outlook Express (DBX)
- □ Exchange (EDB)
- □ Lotus (NSF)
- □ AOL
- □ MBOX
- Additional Options
- ☑ Verify file signatures
- □ Identify codepages
- □ Search for internet history
- □ Comprehensive search

Figure 7b: using Encase or digital analysis (Filtering the evidence)

Forensic Toolkit (FTK)

This is another tool used for digital investigation of a compromised system, used particularly for evidence processing (see diagram below).


Detailed Options
Evidence Processing
Evidence Discovery Options
Evidence Refinement (Advanced)
Index Refinement (Advanced)

Evidence Processing

Select additional data you wish generated during pre-processing.

Generate File Hashes (flag duplicates)

- ☑ MD5 Hash
- ☑ SHA-1 Hash
- ☑ SHA-256 Hash
- □ Fuzzy Hash
- □ Match Fuzzy Hash Library
- □ Flag Duplicate Files
- □ KFF
- □ Expand Compound Files (Email, OLE, ZIP, etc.)
  Takes extra time to extract compound files including email boxes, archives, zips, OLE documents, etc.
- ☑ File Signature Analysis
- ☑ Flag Bad Extensions
- □ Entropy Test
- ☑ dtSearch® Text Index
- ☑ Create Thumbnails for Graphics
- □ HTML File Listing
- □ File Listing Database
- □ Data Carve
- □ Meta Carve
- □ Explicit Material Identification
- □ Registry Reports

The icons by the left side help you to view and choose an option to process the evidence

Figure 8: using Forensic Toolkit (FTK) for digital analysis (Filtering the evidence)

- ➢ ***Sift***

According to [29] another tool for digital analysis is the SIFT (SANS Investigative Forensic Toolkit). This is a collection of open source forensic utilities for digital analysis which is available either as a VMware virtual machine or as an ISO image to create a bootable CD. It provides the ability to examine disks and images created using other forensic software. Some of the file systems supported by SIFT include: Windows (FAT, VFAT, and NTFS), Mac (HFS), Solaris (UFS) and Linux (ext2/ext3).

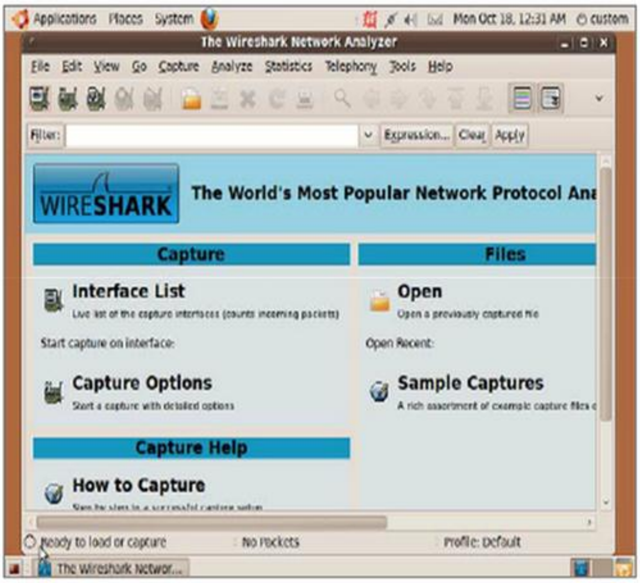

Applications Places System
Mon Oct 18, 12:31 AM
custom
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
WIRESHARK
The World's Most Popular Network Protocol Ana
Capture
Files
Interface List
Live list of the capture interfaces (counts incoming packets)
Start capture on interface:
Open
Open a previously captured file
Open Recent:
Capture Options
Start a capture with detailed options
Sample Captures
A rich assortment of example capture files o
Capture Help
How to Capture
Step by step to a successful capture setup
Ready to load or capture
No Packets
Profile: Default
The Wireshark Networ...

Figure 9: using Wireshark Network Analyser (one of the tools contained in SIFT toolkit)

4. CONCLUSION

Security is what we do to ensure privacy. Securing a computer network or an organization’s information system, would include the protection of its primary assets based on its size, its ownership, the distance it covers and its physical architecture. Consequently, the issue of managing a computer network should include finding solution to major information systems threats. There are basically two sources of information systems threats; Internal and External. Among the external threats and vulnerabilities faced by a computer networks is information system *hack*. Hacking is away to penetrates a network’s security or cause disruption through denial of service attacks, buffer overflows, malware etc. A computer “system” is secured if it is free from worry and if it is safe from threats and vulnerability. However, because we believes that computers constantly communicate with one another; and an isolated computer is crippled, securing a computer system for an application may mean first assuring that the system will be available for use and will deliver uncorrupted information which assures the confidentiality of the information delivered. Basically, if we disconnect our information system from the network it will reduce usability, and if we connect our machine without firewalls or security patches we would make it highly vulnerable. Thus, the issue of computer information security is very vital to organizational goal achievement and the ability to achieve a balance between *usability* and *security* is the major concern of an information system owner.

5. REFERENCES

[1] Shinde, S.S. (2009) Computer Network. Daryaganj, Delhi, IND: New Age International, pp 46. [Available online at http://site.ebrary.com/lib/uoh/Doc?id=10367725&ppg=6. Viewed 14th October 2012.

[2] Peterson, L. L. and Davie, B.S. (2012) *Computer networks: a systems approach.*Amsterdam: Morgan Kaufmann.

[3] Cerf, V.G. (1991) "Networks", *Scientific American*, vol. 265, no. 3, pp. 72-81.

[4] Gollmann, D. (2011) *Computer security*, Wiley: Chichester.

[5] Bosworth, S., Kabay, M.E. and Whyne, E. *eds*. (2012) Computer *Security Handbook.* US: Wiley.

[6] Bishop, M. (2003) "What is computer security?" *IEEE Security & Privacy Magazine*, 1 (1), pp. 67-69.

[7] Whittaker, J.A. and Andrews, M. (2004) "Computer security", *IEEE Security & Privacy Magazine* 2 (5) pp. 68-71.

[8] Murthy, C.S.V. (2010) Data *Communication and Networking.* New Delhi: Himalaya Publishing House.

[9] Peterson, L. L. and Davie, S. Eds (2007) Computer Networks: A Systems Approach (4th Edition). Burlington, MA, USA: Morgan Kaufmann,pp 2 online available on [14th oct 2012] http://site.ebrary.com/lib/uoh/Doc?id=10382874&ppg=31

[10] Newman, R.C. (2010) *Computer security: protecting digital resources.* Sudbury, Mass: Jones and Bartlett Publishers.

[11] Landwehr, C.E. (2001) "Computer security", *International Journal of Information Security.* 1 (1), pp. 3-13.

[12] Vacca, J.R. (2010) *Network and system security.* Burlington, MA: Syngress/Elsevier.

[13] Simpson, M. T., Kent, Backman. and James, E. C. (2012)"Chapter 6 - Enumeration". *Hands-On Ethical Hacking and Network Defense*. Cengage Learning. [Online] Available at *http://common.books24x7.com.libaccess.hud.ac.uk/toc.aspx?bookid=46364* [Accessed November 25, 2012]

[14] Erickson, J. (2007) *Hacking: The Art of Exploitation (2nd Edition),* No Starch Press, Incorporated.

[15] Barber, R. (2001) "Hacking Techniques The tools that hackers use, and how they are evolving to become more sophisticated", *Computer Fraud & Security.* 2001 (3), pp. 9-12.

[16] Graves, Kimberly. (2010) CEH : Certified Ethical Hacker Study Guide. Hoboken, NJ, USA: Sybex. [Online] Available at < http://site.ebrary.com/lib/uoh/Doc?id=10383604&ppg=154> [Accessed 5th December 2012]

[17] Dhanjani, N., Rios B., and Hardin B. (2009) *Hacking: the next generation.* US: O'Reilly.

[18] Barker, W., Beau, H. and Gene, S. (2010) *Network Scanning, Intrusion Detection, and Intrusion Prevention Tools.* Berkeley, CA: Apress. [Online] Available at *<http://common.books24x7.com.libaccess.hud.ac.uk/toc.aspx?bookid=35387>* [Accessed November 19, 2012]

[19] Gibbs, M. (2012) “Google Around, Network Scanning, and Pinging With TCP” *Network World.* 29 (8), p. 16

[20] Darril, G. (2011) *Microsoft Windows Security Essentials.* Hoboken NJ, USA: Sybex Inc, US. pp. 151. [Online] Available at < http://site.ebrary.com/lib/uoh/Doc?id=10484740&ppg=177> [Accessed 24th Nov. 2012]

[21] Mcclure, S., Scambray, J., and George, K. (2005) *Hacking Exposed: Network Security and Solutions*. Emeryville Calif: Mcgraw Hill. [Online] Available at <Http: common books. Books 24x7.Libaccess.hud.ac.uk/toc.aspx?bookid=18191> [Accessed 25th November 2012]

[22] Kennedy, D., O’Gorman, J., Kearns, D. and Aharoni, M. (2011) *Metasploit: the penetration tester's guide*.No Starch Press: [Online] Available at *<http://common.books24x7.com.libaccess.hud.ac.uk/toc.aspx?bookid=43618>* [Accessed 25th November 2012]

[23] Seymour, B., Kabay, M. E. and Whyne eds. (2009) "Chapter 21 - Web-Based Vulnerabilities". *Computer Security Handbook, 7th ed.* John Wiley & Sons. [Online] Available at *http://common.books24x7.com.libaccess.hud.ac.uk/toc.aspx?bookid=29816*> [accessed November 25, 2012]

[24] Cowan, C., Wagle, P., Pu, C., Beattie, S. and Walpole, J. (2000) "Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade," paper presented at DISCEX 000, January 25–27, 2000, Hilton Head, S.C. *Proceedings of the DARPA Information Survivability Conference and Exposition* (Los Alamitos, CA: IEEE ComputerSociety Press, 2000).

[25] Steven, H. and Marah, B. eds. (2010) Ethical Hacking and Counter measures: Attack Phases. US:EC-Council

[26] Stewart, M. (2011) Network security, Firewalls and VPN. US: Jones and Bartlett Learning LLC

[27] Sutherland, S. (2009*) Windows Privileged Escalation Part 2: Domain Admin Privilege*. [Online] Available at < http://www.netspi.com/blog/2009/10/05/windows-privilege-escalation-part-1-local-administrator-privileges/ > [Accessed Dec7 2012].

[28] Oriyan, S-P. and Gregg, M. (2010) Hacker Techniques, Tools and Incident Handling. US: Jones and Bartlett.

[29] Solomon, M, G., Rudolph, K., and Tittel, Ed. (2011)Computer Forensics JumpStart (2nd Edition).Hoboken, NJ, USA: Sybex. Pp. 19 [Online] Available at < http://site.ebrary.com/lib/uoh/Doc?id=10510709&ppg=19> [Accessed 7th Dec. 2012]

[30] Obialero R (2006) Forensic Analysis of a Compromised Intranet Server. SANS Institute [Online] Available at < http://www.sans.org/reading_room/whitepapers/forensics/forensic-analysis-compromised-intranet-server_1652> [Accessed 7th Dec 2012]

[31] Jovanovic, Z., and Redd, I. D. D. (2012) "Computer Forensics Investigation Phases." *Journal of Digital Evidence.* 2 (2), pp. 1 – 20.

[32] Blotzer, M. J. (2000) "Computer security", *Occupational Hazards.* 62 (5), pp. 99.

[33] Harrington, J.L. (2005) *Network security: a practical approach:* Morgan Kaufmann Publishers, Amsterdam.

[34] Rowlingson, R. (2011) *The Essential Guide to Home Computer Security,* BCS. Swindon: The Chartered Institute for IT.