Analysis of Freeware Hacking Toolkit

Albert K. Ansah *Member, IAENG*, Janus Kyei-Nimakoh, Millicent Kontoh

***Abstract*—Computer networks are constantly under threats from intruders affectionately called hackers. This paper looks at assessing the extent to which the Internet abounds in easily accessible freeware computer security tools and online resources which can facilitate unauthorised computer network intrusions. The current position of open source computer network security tools, computer operating systems' vulnerabilities and vendors' responsibility towards their customers would be covered in this paper. The paper also looks at a couple of freeware computer security tools and a handful of computer system vulnerability websites as well. A virtual computer network environment was setup to demonstrate how some computer security tools can be exploited for malicious purposes. A survey to solicit opinions on freeware computer security toolkit was commissioned to ascertain the extent to which respondents use computer security freeware. The concept of some companies trading in computer system exploits would be explored by this paper. An appraisal of a few groups behind the development of some of these freeware computer security tools i.e. hacking tools and why the need for these tools would be also explored. Suggestions of possible defensive countermeasures against malicious use of hacking freeware computer tools would be touched upon. The paper is to inform and educate ICT professionals to be very heedful and pay mindfulness to suggested defensive countermeasures.**

***Index Terms*— Computer Security, Freeware Hacking Toolkit, Intrusion Detection Systems, Malicious Codes, Open Source Software, Operating System Vulnerabilities.**

I. INTRODUCTION AND BACKGROUND

Freeware classifies software that is ready and available for use for an unlimited time at no cost at Free Software Foundation website http://www.fsf.org/. The program source codes are not available. However, open source software license backed by Open Source Initiative (OSI) goes further to make software available for users with source codes included; http://www.opensource.org/. This gives the user the free will to make modifications and enhancements as well as redistribution of the software. It is now common for freeware and open source software users to simply access websites or queries search engines and download source codes and software from bonus compact disc added to books for distribution. A good number of computer network security tools have been developed with either of the above mentioned characteristics, belonging to freeware, open source software genre, or commercial variety. Several malicious intentions culminate in the exploit of some freeware computer security tools. It is much easy to download and install full versions of computer network hacking tools off the Internet to cause mayhem.

Manuscript received May 04, 2012; revised June 19, 2012.

A. K. Ansah is with the Computer Science and Engineering Department of University of Mines and Technology, Tarkwa, P. O. Box 237 Ghana (phone: +233 264 518866; fax: +233 3123 20306; email; afkansah@geologist.com)

J. Kyei-Nimakoh is with Information Technology Department of Central Bank of Ghana, Accra (email: janusenator@gmail.com)

M. Kontoh is with the Computer Science and Engineering Department of University of Mines and Technology, Tarkwa, P. O. Box 237 Ghana (email: millikon2001@yahoo.com)

http://neworder.box.sk for example, has lists of computer system exploits including detailed information on how to identify vulnerable computer systems and the code to launch a computer intrusion attack. This website publishes large host of articles on hacking techniques, computer exploits tools, discussions on latest software vulnerabilities, user message boards discussing computer intrusion techniques, questions and answers linked to computer security and networking. The ambition of the website is supposedly to educate and advice administrators of computer network systems. It is intriguing to notice that open source and freeware hacking toolkit are always freely accessible from the Internet. Some computer security professionals belong to the school of thought: that security by obscurity principle (Preetham, 2002) is the best option to implement secure computer network security. In a preliminary research, it was discovered that, there exist some software tools categorized as vulnerability scanners or vulnerability assessment tools. There are some computer enthusiasts who trawl the Internet looking for vulnerable computer networks very frequently. Indecorously configured networks may be exploited by malicious computer network resources into their concourse.

A distinctive example of a vulnerability scanner program that supports Linux, FreeBSD, Solaris, Mac OS X and Windows platforms is Nessus which may be freely downloaded from http://www.nessus.org/download. Adopting security by obscurity principle alone may not be enough unless used with other network security policies (Preetham, 2002). SIMPLE Internet queries on Google for "open source remote network administration tool" returns several results with details of other tools including the Back Orifice tool. The dual purpose of some these computer network tools makes it imperative for network administrators to be more vigilant of the list of software installed on their network. This paper is not vying for a restriction to open source or freeware network security tools. It rather seeks to raise awareness vis-à-vis the threats they (freeware network security tools) may pose and suggesting appropriate countermeasures. This paper is to inform and educate ICT professionals to be heedful and pay mindfulness to suggested defensive countermeasures.

II. FREEWARE COMPUTER SECURITY TOOLS

A Software tool may be a piece of software utility that can be used to carry out a particular task or computer system maintenance task. A computer network packet sniffer is a software tool used for network packet sniffing purposes. Information technology tools could be either offensive or defensive; some are used for both purposes. It is therefore necessary that network security inclined tool be a required utility which may be occasionally needed for network maintenance. In Information Security, software tools may be used for network penetration testing exercises, network vulnerability reviews, Intrusion Detection Systems *(IDS)* monitoring, network troubleshooting or network monitoring tasks. Penetration test (sometimes referred to as ethical hacking) is a technique of evaluating the level of security of

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

a computer network by simulating a network intrusion by a malicious user. This exercise is conducted (with consent of system owner) by authorised computer security professionals (Clure et al., 2005) and very often involves the use of some freeware or open source network security tools. The process involves an active analysis of the system for any potential vulnerability that may result from poor system configuration, hardware or software flaws and is carried out from the position of a potential attacker, and very often involves the effective exploitation of network security vulnerabilities. The primary reason why a penetration test is carried out is to chiefly discover vulnerabilities in the target computer system and fix them before an attacker does.

Nmap may also be used for penetration testing and has a dual purpose of attacking or defending a computer network setup. Nmap and Nessus security tools have legitimate uses in the administration of networks and are freely available over the internet. Penetration testing is the process of attempting to gain access to network resources without knowledge of usernames, passwords and other normal means of access. Penetration testing aims to find vulnerabilities and fix them before a malicious guru or hacker does. In an article (Anderson, 2007); it was revealed that in 2007, Germany outlawed "hacking tools". Computer network system is certified secured after first using software to attempt to break-in or carry out an audit of security vulnerabilities present in the computer network system. In fact there are several software that can be used for both legitimate auditing and potentially criminal conduct. The dual purpose characteristics of open source computer security toolkit are a mixed blessing; because they may be used for both computer network auditing or malicious intentions.

Thousands of open-source security tools are available for download. www.freshmeat.net has over 1,200 open source security projects and www.sourceforge.net has over 3,300 on-going open security projects (Harvey, 2007). Using open source tools allow users to fine tune their security solution to meet their needs and to modify or adapt solution as and when their system needs evolve. Since open source is freely available, it is easily accessible and an attractive option as opposed to commercially available ones which may be very expensive. Computer network security tools come in different types (Fyodor, 2007). Some are password crackers or recovery tool, vulnerability assessment scanners, rootkit detectors, encryption tools, web scanners, wireless discovery tools, port scanners, OS detection tools, vulnerability exploitation and network packet sniffer tools. Fascinatingly, the popular search engine Google; www.goolge.com is progressively being used to search for information about a target company's or as a security testing tool; this is called Google hacking (Long, 2005).

A. OPERATING SYSTEM (OS) VULNERABILITIES

Major Operating Systems *(OS)* have design flaws, weakness or vulnerabilities intrinsic within them. Certain vulnerabilities are caused by a narrowly missed design over sight or simply errors in the handling techniques employed by the OS in question (Singh, 2006). System flaws can be taken advantage of by malicious gurus to launch security intrusions (Singh, 2006). Vulnerabilities could be launched locally or remotely across a computer network. Security patches have become part of purveyor responsibility towards end users. Patch Tuesday, thus regular security patching cycle is the second Tuesday of each month. This is the day Microsoft releases vital security patches, fixes and updates (Barber et al., 2005). End users rely on this security updates to secure their computer systems. Certain software vulnerabilities are publicly known to information security professionals. A malicious guru could abuse a computer program by taking advantage of the discovered vulnerabilities, by simply executing some commands. Sensitive data on the target system can be stolen, modified or even deleted by the intruder (Singh, 2006).

Many open source or freeware tools discovery and identifying *OS* vulnerabilities exist. A typical example is Nessus vulnerability scanning software tool; freely accessible at http://www.nessus.org/download/. The regular application of software patches, use of firewalls and implementation of sound computer network security policies can reduce the prevalence of a vulnerability being exploited. In information security circles, zero-day (0-day) exploits are vulnerability exploits which vendor patches and respective exploit details are released to general public & published on dedicated website or newsgroups the same day (Long, 2005). A website that provide resource platform on the Internet dedicated to security tools creation and exploits distribution is http://framework.metasploit.com/. The ground breaking framework allows the user to configure an exploit module and launch it at a target system.

B. INTRUSION DETECTION SYSTEMS (IDS)

Intrusion Detection Systems were developed to detect and monitor unauthorized and malicious computer network intrusions. *IDS* are network security monitoring tools used to check and reveal numerous variations of malicious computer network traffic otherwise called security breaches. They are basically used to find out people trying to get into networked systems. Attackers always try to sidestep any *IDSs* installed on a network. Hackers may use various different techniques to fool *IDSs* by forging data packets to make them look genuine to the IDSs. An *IDS* uses a system of rules to issue alerts from security events recorded. *IDSs* are made up of sensors to produce security events, a console to keep an eye on events and alerts. *IDSs* come in two main types; hostbased intrusion detection system *(HIDS)* and network intrusion detection system *(NIDS).* Some *IDSs* are Hybrids of these two. *NIDS* captures and scan data flowing on a network for malicious traffic. Snort, freely accessible at http://www.snort.org is an example of an open source *NIDS* (Cox and Gerg, 2004). *HIDSs* are installed on particular hosts and detect attacks targeted to that host only (Shinder, 2003). The following major mechanisms; Packet Decoder, Pre-processors, Detection Engine, Logging and Alerting System and Output Modules make up Snort (Rehman, 2003).

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

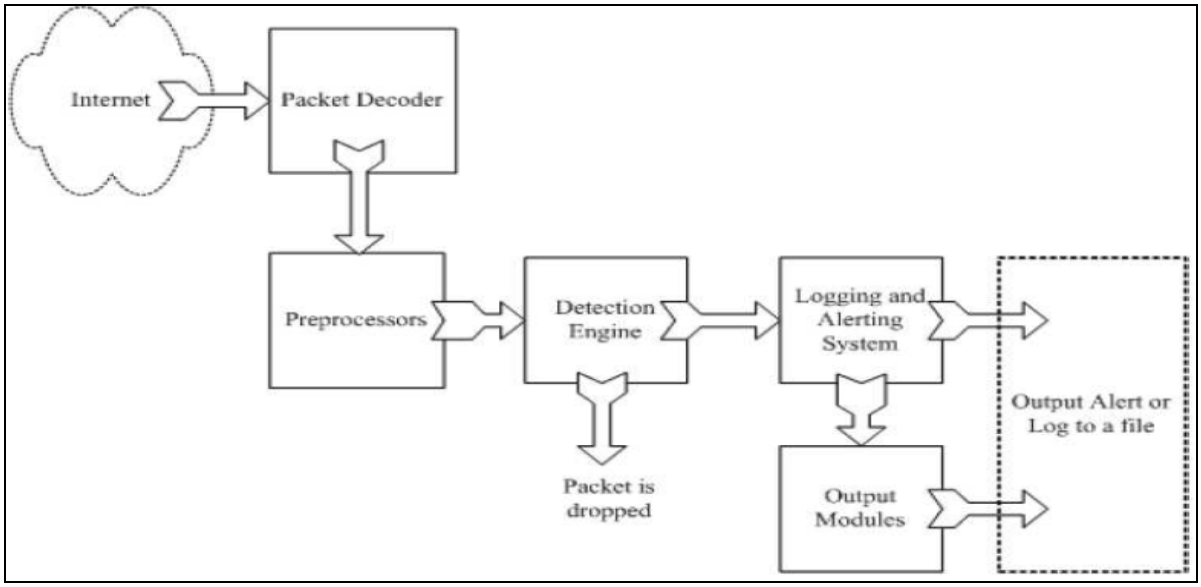


Figure 1: Components of Snort diagram. (Rehman, 2003)

III. BRIEF HISTORY OF THE WORD HACK

Hack was coined at Massachusetts Institute of Technology *(MIT)* school campus in the 1960's. Hack meant a witty way of doing things. Hackers at *MIT* originally aimed to make electric trains to perform faster and more efficiently. Group of these hackers later decided to try their hacking prowess on the computer mainframes of the *MIT* http://news.bbc.co.uk/1/hi/sci/tech/994700.stm. Hacking is now hijacking or breaking into any kind of computer or telecommunications system. Hackers discover and may take advantage of exploits in computer systems. In the context of network security, an exploit refers to a piece of software or sequence of commands that take advantage of vulnerability in a computer system. Some of the common types of exploits include the following; Buffer overflow, Heap overflow, Integer overflow, Return-to-libc attack, Format string attack, Race condition, Code injection, SQL injection, Cross-site scripting and Cross-site request forgery. The hacker may further snip or gain access to unauthorised information after the break-in. Phone hackers also known as phreaks may break into regional and international phone networks to make free calls. This is regarded as a form of hacking. It should be noted that Hacking is not limited to computer break-in only but covers tinkering with the capabilities of any electronic device. In the 1980s, Phone phreaks began to shift to computer hacking as well, just about the time the first electronic Bulletin Board Systems *(BBSs)* began to develop. BBSs are similar to the yahoo groups of today where users posted messages or topics of any interest. As a result of the growth of the Internet around the world, hackers' numbers and activities have multiplied and the subject is being discussed in mainstream electronic media these days regularly. Phreaks and hackers used BBS to gossip, discuss how to break into systems, trade tips and credit card numbers. Now, it is Security professionals who discuss how to break into systems in public places and high profile conferences. BBSs are now replaced by the Internet. There are several websites dedicated to hacking and tools related to hacking. This information is accessible and may be freely downloaded from the Internet.

A. MOTIVES OF HACKING

Certain group of hackers referred to as Hacktivists have been responsible for many web defacement and attacks of websites for political reasons in the past. Some of their victims are groups of people who are against their ideologies. Hacktivismo for instance, is one of such groups of Hacktivists. They can be found at http://www.hacktivismo.com/index.php. It is an organisation that has evolved out of the group. Some reasons and motives of hack attacks may be intelligence gathering by some law enforcement departments, stealing program source codes, financial gain i.e. stealing people's identity details to impersonate them and commit fraud, bragging rights i.e. in order to gain reputation among peers, gaining access to unauthorised information, thrill, political hacktivism i.e. by promoting some ideologies, fun of hacking sake etc. (Sagar and Chakrabarty, 2003).

Any group of people can organise themselves into Hacktivists bearing in mind the fact that hacking tools may be easily downloaded off the Internet freely. The fact is computer network security tools that are used for finding security flaws in websites and computer networks may sadly be used to launch successful hacking attacks on targeted computer networks as well. Open source software has no copyright licensing restrictions on them and they are fully functional software programs too.

IV. METHODOLGY

An exploration of some freeware computer network security tools with VMware version 6.0 http://www.vmware.com/products/ws/ and an online survey of internet users on freeware computer network security tools was conducted. Respondents were invited to take part in the online survey from several online mailing lists. Virtual machine was created on host computer using VMware version 6.0 for the freeware computer network security tools for analysis. In order not to default any legal act, a virtual machine with a virtual computer network was used to explore the various computer security tools. For the simulation of malevolent use of the network security tool, Windows *XP* Professional virtual machine was created using VMware version 6.0 ACE edition on a Microsoft Windows

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

XP Home Edition laptop. Nmap tool has been installed on the Windows XP Professional virtual machine. Nessus vulnerability scanner from tenable was also installed on the Windows XP Professional virtual machine. VMware has better support for computer virtual networking features including Bridged, NAT, host-only and custom virtual network settings and a built-in *DHCP* sever http://www.vmware.com/files/pdf/ws_datasheet.pdf.

Nmap uses Internet Protocol *(IP)* addresses to accomplish its target scans successfully. The ping utility sends data packets to the recipient computer using the *ICMP* echo command and if the recipient computer is present a response is given to the sending computer stating ping was successful. A successful ping confirms the two computers are able to communicate (Casad, 2004). For instance, running the ping command on www.acp-estates.com at the command prompt on a computer with an active internet connection returns an ip address of 64.202.163.147. This ip address can be used in the Nmap scan. It must be appreciated here that no live ip addresses were used in the demonstration for legal reasons.

The procedure described here could be used to deface any website, that is, this simply involve replacing a file on the web server with another one created by the computer network intruder after breaking into the victims computer network. It could also be used to get credit cards details of innocent people from the compromised machine, get hold of passwords, obtain source code and may obtain email record details illegally. After breaking in, the intruder may conceal their presence from the operating system by using rootkit software. Nmap was run from the Microsoft Windows *XP* professional virtual machine against the host machine; Microsoft Windows *XP* Home Edition platform laptop. It took about eighteen minutes in the demonstration to get the results displayed onscreen.

A simple Nmap scan results tell the characteristics of the target computer such as open ports and ports that have tcp protocol running on them. Exploits and vulnerabilities related to these ports can be found out at several security web sites. An enhanced probe for a more detailed output can be done with the *-vv –sS –sV* scanning techniques. -vv specifies the verbosity levels of the results of the scan and –sS launches a *SYN* Scan. It also tries to determine what operating system is running on each host that is up and running. To determine what application is running on the target system, –sV Version detection is used. The scan command against the target computer using Nmap 192.168.1.3 -vv –sS –sV (Figure 3) shows more about the target computer.

The results from 192.168.1.3 -vv – sS –sV (Figure 3) shows that the target operating system has Microsoft Windows XP running, port 110 is open with tcp protocol running by an application called *AVG* and pop3-proxy is a service running on that port as well. The results go on to list all open ports found during the scan. From the results, ftp protocol running on Port 912 which is open. Running Nessus vulnerability scanner against the host's ip address reveals a lot of vulnerabilities on the target host computer. In this demonstration, however, the host machine which is a Microsoft Windows XP Home Edition laptop is the host being scanned using Nessus. The scan was executed from the windows XP professional virtual machine. A snapshot of Nessus in action is shown in Figure 4.

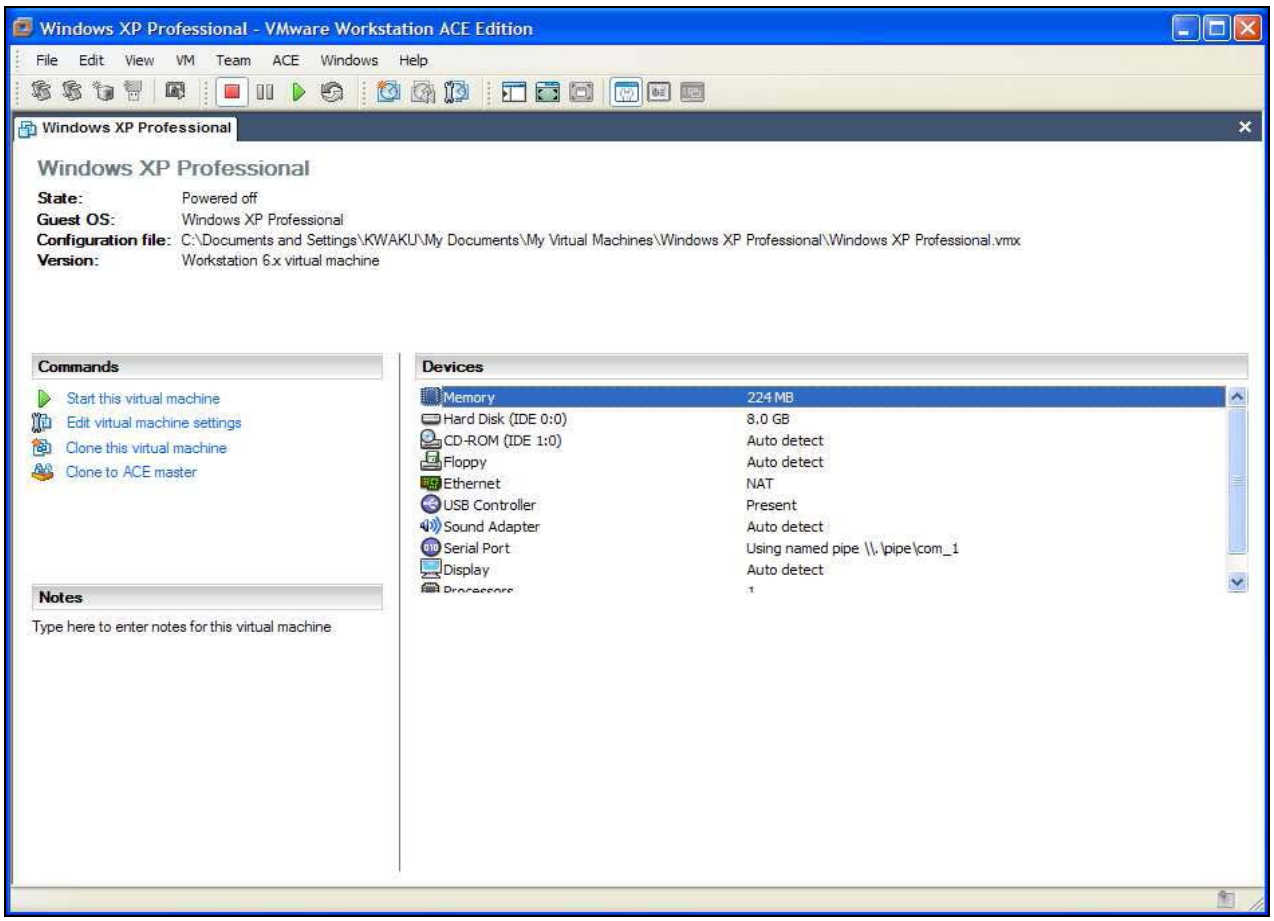


Figure 2: Virtual machine with Windows XP Professional installed

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

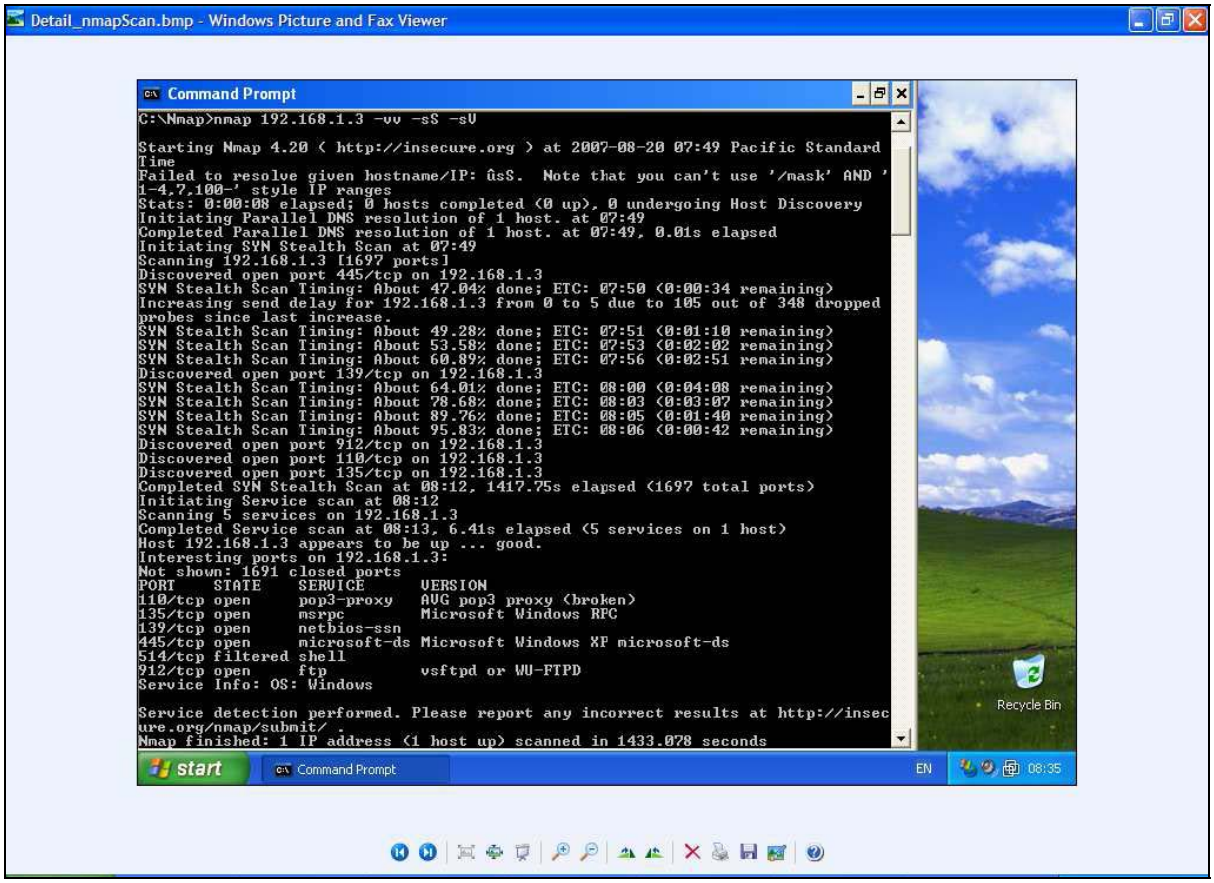


Figure 3: A snapshot of the scan results after using the command: Nmap 192.168.1.3 -vv –sS –sV

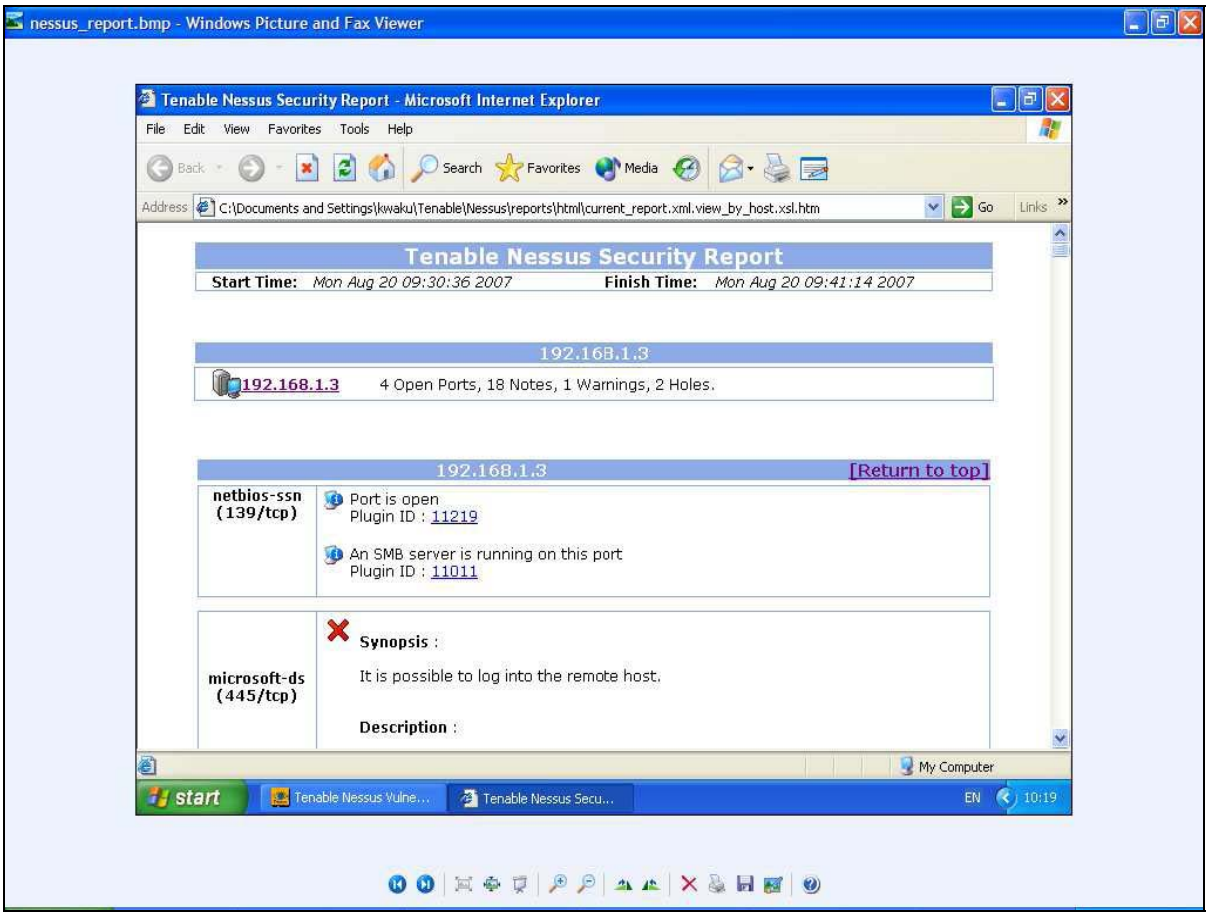


Figure 4: Results of a Nessus scan

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

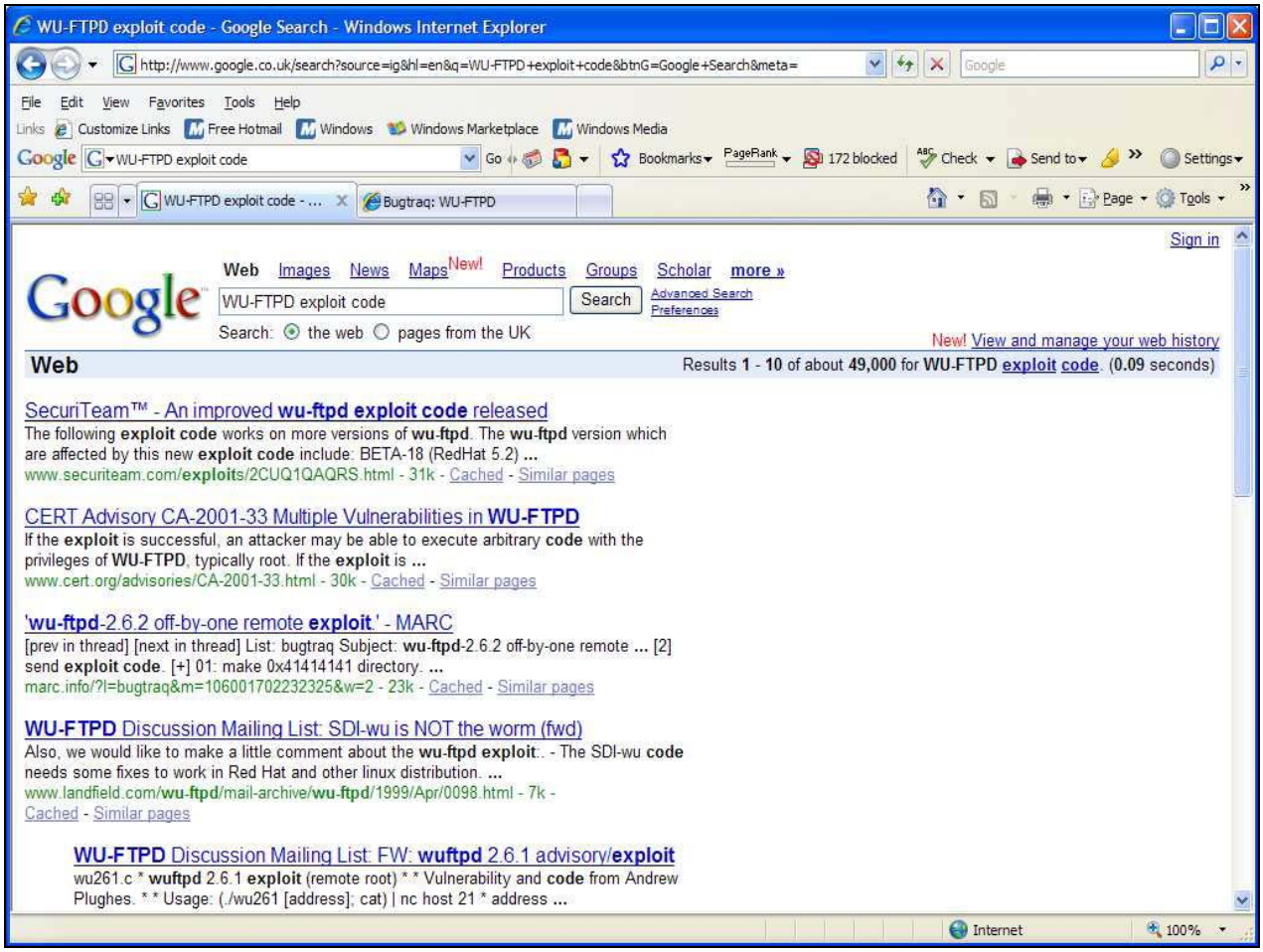


Figure 5: Results of 'WU-FTPD exploit code' from http://www.google.co.uk

Under the Microsoft-ds (445/tcp) column Synopsis, the report states that, it there is a possibility to access a network share. It describes that the remote has one or many Windows shares that can be accessed through the Network. It may allow an attacker to read/write confidential data depending on the share rights. The Nessus user gathers a wealth of information of vulnerabilities about the target computer system at this stage. A simple search on Google can be done to reveal exploits and vulnerabilities associated to the operating system running on the target machine. Since it is already known that the host is running Microsoft Windows XP, WU-FTPD exploit code was typed into http://www.google.co.uk. A host of information relating to various WU-FTPD exploit codes were displayed in the results as seen in Figure 5. On the top of the results list is an article entitled 'An improved wu-ftpd exploit code released' which is written by securiteam. Within the article is a full source code for the exploit. This exploit can easily be compiled and be used in attacking any host identified with the WU-FTPD vulnerability.

This website has the full listing of the script source code http://www.securiteam.com/exploits/2CUQ1QAQRS.html. The script source code could be compiled in a 'C' compiler in order to get it working. However, the 'C' compilation element is not demonstrated in this paper. Exploits are sometimes written using Perl scripts as well. After running the compiled exploit against the target machine the intruder may easily gain access to the victims' computer network. This feat was all achieved using freeware computer security tools and online computer security resources, together with a lot of patience. This highlights the threat computer network security tools may pose when they are used irresponsibly.

Access to sensitive data on targeted machines is possible. Earlier from the much detailed Nmap scan, it was discovered that pop3-proxy is a service running on port 110. Therefore one may decide to look for exploits or vulnerabilities related to pop3-proxy. In that case pop3-proxy may be input into the search box on the Google or security focus website. Some dedicated computer vulnerability websites like securityfocus website http://www.securityfocus.com/vulnerabilities have wealth of information on computer exploits and how to set up a Trivial File Transfer Protocol *(tftp)* transfers to replace files on the targeted computer thereby achieving website defacement. Trivial File Transfer Protocol *(tftp)* is very simple file transfer protocol used to perform send and receive operations in client server architecture (Kozierok, 2005).

A. SURVEY

To determine the prevalence and the use of freeware computer security tools, an online anonymous survey was utilised. The concept behind the survey was to discover new computer network security tools. The primary objective is to get respondents to share their favourite freeware or open source computer networking security tools. The questionnaire was hosted on Survey methods website; http://www.surveymethods.com. Survey methods came out as best option for hosting the survey because their website had full featured survey software that is easy-to-use. Survey methods also had a feature which prevents respondents from

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

taking the survey twice. An IT Security mailing list consisting of IT Security Professionals where invited to partake in the survey. It takes about three minutes to complete and submit the survey (Appendix I). On the whole, twenty (20) responses were received within a fortnight. Some of the questions asked the respondents to list any of their favourite Open source or Freeware computer network security tools. This question was included in the survey to discover more computer network security tools. The question 'do you intend to collect and explore more Open source or Freeware network security tools' was asked to find out how many freeware tool users would carry on to collect and explore despite the threat they pose. Thus when these tools fall into the hands of malicious users, they can carry out unauthorised computer intrusion with them.

B. LEGAL AND ETHICAL CONCERNS OF METHODOLOGY

The computer intrusion experiment has a lot of legal and ethical implications. Under Section 1 of the Computer Misuse Act 1990 in the United Kingdom, a person is guilty of an offence if he carries out an unauthorised access to any computer system. The law under section 1 of UK's Computer Misuse Act 1990 states as follows:

A person is guilty of an offence if -

a. He causes a computer to perform any function with intent to secure access to any program or data held in any computer;

b. the access he intends to secure is unauthorised; and

c. He knows at the time when he causes the computer to perform the function, that is the case.

In order not to fall foul of the Computer Misuse Act 1990 law, a virtual machine with a virtual computer network was used to explore the various computer security tools.

V. ANALYSIS

Out of twenty respondents who participated in the online survey, nineteen fully completed the survey with one partial completion. Appendix II shows snap shots of sections of survey questions' and respondents graphs. Seven (7) respondents corresponding to 35% described themselves as *IT* Security Enthusiasts and eight (8) corresponding to 40% said they were IT Security Consultants. Results from the survey suggest the highest number of respondents were between the ages of 21 and 30 years, thus 35%. The next higher age group is between 31-40 years making 30% of the total respondents. 100% of the respondents were males. On the question of 'what organisational level do respondents work at currently', 40% answered Network administrators, 15% Penetration testers and 5% unemployed. 80% of respondents use some type of Freeware computer network security tool while 20% said the contrary. 75% of respondents said they use some type of Freeware computer network defensive security tools and 25% said no. 55% of respondents said they use some type of Freeware computer network attack security tools and 45% said no. 65% of respondents said they Stumble upon the Freeware computer network tools they use from an Internet search. This suggests a greater number of freeware computer security tools are available on the Internet. 45% got to know of the computer network tool from Peers and 15% from academic sources. Other sources cited were IT security conferences and SANS.

Respondents gave the following as their favourite freeware computer network security tools; Nmap, Nessus, hping, wireshark, Unicom scanner, Snort, Backtrack, Metasploit framework, zone alarm, superscan3, PCTools, Sandboxie, Comodo, firewall pro, honeynet, iptablse/netfilter, spamassassin, airsnort, Aircrack-ng, linux/netfilter, openbsd/pf, filetraq, tripwire, tcpdump, prelude, nikto, arpwatch, arpstar, pfSense, OpenBSD, PGP, Enigmail, Truecrypt, DSniff, FPing, Ollydbg, netwox, airsnarf, netcat and Ossec. 35% expressed readiness to join user group to learn more or share their interest in any freeware network security tool. 15% do not intend to join any user group while 25% are undecided yet, and 25% are very likely to join. This suggests a high level of interest in freeware network security tools from respondents. 85% said '*Yes*' to plan to carry on to collect and explore more freeware network security tool and 15% said '*No*'. The percentage figures above are with respect to individual questions. In summary, respondents shared their opinions on freeware computer security tools they use. Numerous computer security freeware tools have been unveiled to the authors as a result of the survey. The actual number of respondents was much lower than expected.

A. SCRUTINY OF VIRTUAL COMPUTER NETWORK EXPERIMENT

The motivation to breach the security systems on a computer network may be a computer intruders' drive and for some intruders it is to enhance their reputation, thus sense of achievement among their peers (Bainbridge, 2004). The Nmap security tool was used in the computer network intrusion attack demonstration. The *XP* professional virtual machine was deployed as a source machine for the intrusion. A virtual network was set up between the virtual machine and the host Microsoft Windows *XP* Home Edition laptop in other not to break computer misuse act as in the case of Daniel James Cuthbert (Oates, 2005). Nmap scans works on both remote and local machines http://insecure.org/nmap/. Even though the Windows XP professional virtual machine was in direct network with the host machine, the network was used to simulate two machines wired to each other over the Internet. The similarities of the Internet to the virtual network used is that, on the Internet each machine has an ip address and the interconnected machines can talk to each other using the internet protocol (Kozierok, 2005).

The ping command utility, a built-in tool within the Microsoft Operating System *(OS)* for network administration tasks (Casad, 2004) was also exploited. Nmap scan results displayed lots of information from *OS* type to open ports on the target machine depending on the Nmap scanning option used. Nessus vulnerability scanner was used next, http://www.nessus.org. Nessus is legitimately designed for the network administrator to assist them in finding vulnerabilities on their network before the 'bad guy' does. Nessus also revealed incredible detailed report on all vulnerabilities found on the target system. It was fairly easy to search for exploits relating to *OS* and open

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

ports found on the targeted computer network. The exploits found on the Internet had detailed guides to follow, thus how to use the exploits and vulnerabilities effectively. By exploiting freeware computer security tools and consulting online computer security resources, the authors have more than a good chance to be able to exploit a target computer system's vulnerabilities to gain unauthorised access.

VI. CONCLUSIONS

The paper sets out to analyse some freely available hacking software tools, their threats to computer network security. Discussions on the ease of accessibility to some network security tools; freely downloadable from the Internet and an attempt to raise awareness of the vast amount of information freely available on the Internet to compromise computer network security were touched upon thoroughly. It is necessary for network security professionals to install Intrusion Detection Systems (IDS) to monitor and ascertain unauthorized intrusion to their systems since freeware hacking tools are freely accessible on the Internet. The research showed that thousands of open-source security tools are available for download from the Internet.

The paper again reveals that Metasploit framework accessible at http://framework.metasploit.com/ is a flexible and powerful online resource which allows the user to configure an exploit module and launch it at a target system and also to create security tools and exploits. The paper also concludes that by knowing malicious Hackers' techniques, network administrators can combat the menace. The paper goes further to disclose that there are numerous motives for computer hacking which range from stealing people's identity details to impersonate them and commit fraud, through to gaining reputation among peers and promotion of some ideologies (Sagar and Chakrabarty, 2003). An online survey on freeware computer network security tools was carried out. Numerous computer network security tools exist which belong to either the freeware or open source software genre. A site like http://neworder.box.sk has lists of exploits, sections of the web site explicitly talks about the computer exploits and how to use them. Attacker may easily find loops with the aid of some freeware vulnerability scanners. More than a few major Operating Systems (OS) and popular web browsers have design flaws, weakness or vulnerabilities within them. Computer system flaws can be taken advantage of to launch computer network security intrusions (Singh, 2006). Due to legal reasons (Computer Misuse Act of 1990), the authors did not scan any live web sites during the Nmap and Nessus scans. Nmap was run from the windows XP professional virtual machine created earlier against the host machine, which is a Microsoft windows XP home edition platform laptop.

The research discovered ports from the scans used to compromise the security of the target computer in the demonstration. Reliability of research methodology was also considered in the methodology phase. A detailed discussion on legal and ethical concerns which arises as a result of the computer intrusion experiment used as part of the methodology was considered in order not to violate Computer Misuse Act. Respondents of the online survey commissioned on freeware computer security tools revealed a list of freeware computer security tools. Computer network security tools like Nmap and Nessus should be used against users own website for sensitive information or vulnerable files (Long, 2006). Disabling non essential services running on a web server is highly recommended in order to block their exploitation by would be computer intruders. System administrators should properly configure their network using firewalls or routers in order to limit inbound and outbound access to web servers (McClure et al., 2005) and are encouraged to enable logging on their web servers which may later be used to track down and identify computer hackers.

Password creation policies should encourage users to choose stronger passwords in all instances. Computer system administrators are reminded to change default passwords settings on computer devices and equipment (McClure et al., 2005). Installation of anti-rootkits and its regular update of software are highly recommended policies. Intrusion Prevention Systems-IPS and Intrusion Detection System-IDS software should be in place to log and capture all system intrusion attempts for a review by the computer network administrator. It is strongly suggested therefore that computer network security risk assessments, computer network vulnerability testing should be carried out on a regular basis and its corresponding countermeasures be considered and implemented.

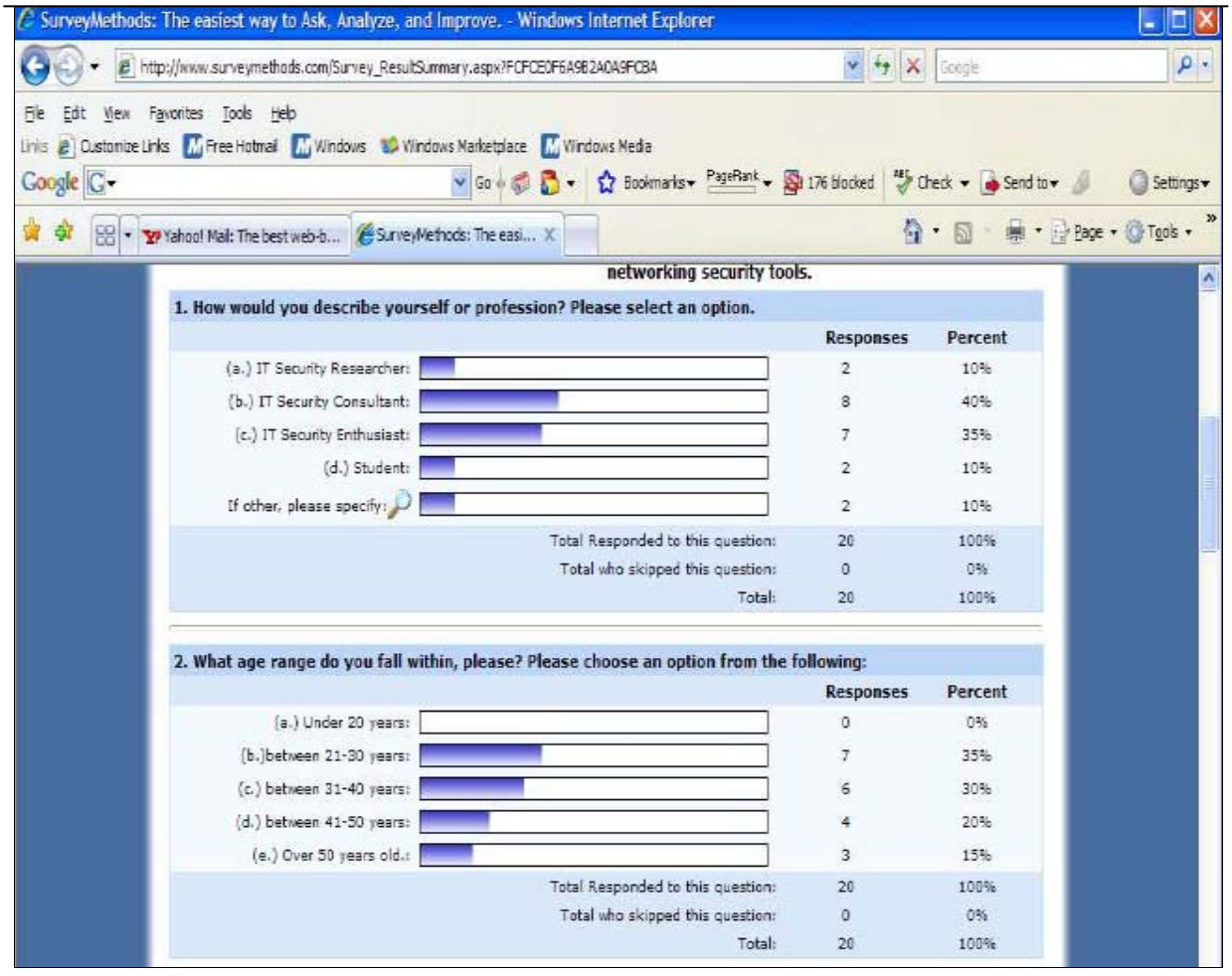
Admins should avoid storing sensitive information on the Internet or web servers totally and sensitive data has to be sent via secure and encrypted emails. Computer network security tools like Nmap and Nessus should be used against users' own website for sensitive information or vulnerable files (Long, 2006). Sensitive Data in web development source codes should be removed to avoid them being compromised. Non-essential services running on a web server should be disabled to combat the scenario where intruders may attempt to take advantage of them. File sharing across networks should be disabled when not required. Services available remotely over the network or locally not required should be disabled immediately (McClure et al., 2005). Network ingress and egress filtering policy should be adopted to limit inbound access to various web servers and outbound communications from the web server. Users should be discouraged from picking dictionary words as passwords or writing passwords on sticky notes & kept under computer keyboards. Intrusion Prevention Systems-IPS and Intrusion Detection System-IDS software should be in place to log and capture all system intrusion attempts (Hoglund, 2006). War driving tool kit and wireless network sniffers may be used to discover open wireless computer networks but a countermeasure is to properly configure the wireless network to block SSID requests (McClure et al., 2005).

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

APPENDIX

The questions below shows what was used in the online survey:

1. How would you describe yourself or profession? Please select an option. (a.) IT Security Researcher (b.) IT Security Consultant (c.) Student (d.) IT Security Enthusiast (e.) other, please specify.
2. What age range do you fall within, please? Please choose an option from the following: (a.) Under 20 years (b.)Between 21-30 years (c.) between 31-40 years (d.) between 41-50 years (e.) Over 50 years old.
3. Gender? Please select an option. (a.) Male (b.) Female
4. What organisational level do you work at currently? Please select an option. (a.) Penetration tester (b.) Network administrator (c.) Unemployed (d.) chief information officer (e.) other, please specify.
5. Do you use any Open source or Freeware computer network security tool? Please select an option. (a.)Yes (b.) No.
6. Do you use any Open source or Freeware computer network defensive security tool? Please select an option. (a.)Yes (b.) No.
7. Do you use any Open source or Freeware computer network attack security tool? Please select an option. (a.)Yes (b.) No.
8. How did you hear about the Open source or Freeware computer network security tools you use? Please select any option that applies (a.) From Peers (b.) Stumble upon it from an Internet search (c.) From Academic sources (d.) other, please specify.
9. Please list any of your favourite Open source or Freeware computer network security tools you use.
10. How would you best describe your favourite Open source or Freeware computer network security tool? Please select any option that applies. (a.) Vulnerability scanner tool (b.) Exploit discovery tool (c.) Security scanner tool (d.) Port scanner tool (e.) Packet filter tool (f.) Other, please specify.
11. Please state on which operating system platforms you run these tools on? For example Linux, FreeBSD, Solaris, Mac OS X or Windows.
12. How ready are you to learn more or share your interest of any Open source or Freeware computer network security tool by joining a User group related to the tool? Please select an option (a.) Do not intend to (b.) Very ready to (c.) Not decided to (d.) Very likely to (e.) Would not join User group
13. Do you intend to carry on collecting and exploring more Open source or Freeware network security tools? Please select an option (a.)Yes (b.) No



ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

REFERENCES

[1] A. Singh, (2006), *Mac OS X Internals: A Systems Approach*, United States of America: Addison-Wesley Professional
[2] A. Lockhart, (2006), Network Security Hacks, Second edition, United States of America: O'Reilly Publishing
[3] A. Sagar and S. Chakrabarty, (2003), *Common Attack methods* [online] Available from: http://www.cert-in.org.in [Accessed June 20, 2011]
[4] A. Savvas, (April, 2007), *TJX hack the biggest in history*, [online] Available from: http://www.computerweekly.com/Articles/2007/04/02/222827/tjx-hack-the-biggest-inhistory.htm Online [Accessed August 6, 2011]
[5] B. Barber, T. Piltzecker, S. Snedaker and C. Todd, (2005), *How to Cheat at Managing Windows Server Update Services*, Canada: Syngress Publishing
[6] C. M. Kozierok, (2005), The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference, United States of America: No Starch Press
[7] Computer Misuse Act 1990- chapter 18, *Computer Misuse Act 1990, chapter 18*, [Online] Available from: http://www.opsi.gov.uk/acts/acts1990/ukpga_19900018_en_1#pb1-l1g1 Online [Accessed Aug. 25, 2011]
[8] C. Harvey, (2007), *Ten Open Source Security Apps Worth Considering* [online] Available from: http://www.itmanagement.earthweb.com//article.php Online [Accessed April 27, 2011]
[9] D. Bainbridge, (2004), *Introduction To Computer Law*, Fifth Edition, Great Britain: Pearson Longman
[10] R. G. Netemeyer, S. C. Sharma, W. O Bearden, W. O. Bearden, (2003), *Scaling Procedures: Issues and Applications*, page 95, USA: Sage Publications
[11] Fyodor, (2007), *Top 100 Network Security Tools* [online] Available from: http://www.insecure.org Online [Accessed June 4, 2011]
[12] Greg Hoglund, (2006), *Rootkits: Subverting the Windows Kernel*, Second edition, United States of America: Addison-Wesley Professional
[13] J. Beale, B. Caswell, J. C. Foster, R. Alder, J. Babbin, A. Doxtater, T. Kohlenberg, M. Rash, and S. Northcutt, (2004), *Snort 2.1 intrusion Detection*, Second Edition, USA: Syngress Publishing
[14] J. Casad, (2004), *Sams Teach Yourself TCP/IP in 24 Hours*, Third Edition, USA: Sams Publishing
[15] John Leyden, (27th Sept., 2006), *Naive 'hacker' escapes punishment*, Online Available from: http://www.theregister.co.uk/2006/09/27/nz_bank_test_trial [Accessed Aug. 25, 2011]
[16] J. Long, (2005), *Google Hacking for Penetration Testers*, USA: Syngress Publishing
[17] J. Long, (2006), *The Google Hacker's Guide - Understanding and Defending Against the Google Hacker*, Online eBook Available from: http://johnny.ihackstuff.com [Accessed Aug. 2, 2011]
[18] K. J. Jones, M. Shema, and B. C. Johnson, (2002), Anti-hacker Tool Kit, First edition, USA: McGraw-Hill Professional
[19] K. M. Mackenthun, and J. I. Bregman, (1992), *Environmental Regulations Handbook*, page 277, USA: CRC Press
[20] Kerry J. Cox and C. Gerg, (2004), *Managing Security with Snort and IDS Tools*, First edition, USA: O'Reilly Publishing
[21] M. Kaeo, (2004), *Designing Network Security*, Second edition, USA: Cisco press
[22] Nate Anderson, (2007), *Germany adopts "anti-hacker" law critics say it breeds insecurity* Online Available from: http://arstechnica.com/news.ars/post/20070528-germany-adoptsanti-hacker-law-critics-say-it-breedsinsecurity.html [Accessed July 8, 2011]
[23] R. Ur Rehman, (2003), *Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID*, First Edition, USA: Prentice Hall PTR
[24] R. A. Zeller and E. G. Carmines, (1979), *Sage University Paper – Reliability and Validity Assessment*, USA: Sage Publications
[25] R. Lemos, (July, 2005), *3Com launches Vulnerability-buying program* Online Available from:http://www.securityfocus.com:80/news/11253 [Accessed August 7, 2011]
[26] R. Slade, (2006), *Dictionary of Information Security*, Canada: Syngress Publishing.
[27] *An improved wu-ftpd exploit code released*, Online Available from: http://www.securiteam.com/exploits/2CUQ1QAQRS.htl [Accessed Sept. 16, 2011].
[28] *Microsoft Windows Graphics Rendering Engine MF SetAbortProc Code Execution Vulnerability*, Online Available from: http://www.securityfocus.com/bid/16074/discuss [Accessed Nov. 6, 2011]
[29] Stuart Mc Clure, Joel Scambray, George Kurtz, (2005), *Hacking Exposed: Network Security Secrets & Solutions*, Fifth edition, United States of America: McGraw-Hill Professional.
[30] Thomas W. Shinder, (2003), *The Best Damn Firewall Book Period*, United States of America: Syngress Publishing.
[31] V. V. Preetham, (2002), *Internet Security* and Firewalls, United States of America: Premier press.

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)