International Journal of Computing Sciences Research (ISSN print: 2546-0552; ISSN online: 2546-115X)
Vol. 5, No. 1, pp. 407-425
doi: 10.25147/ijcsr.2017.001.1.49
https://stepacademic.net

Short Paper

Security Auditing Tools: A Comparative Study

Saria Islam
Assistant Professor (Computer Science and Engineering)
School of Science and Technology
Bangladesh Open University
saria_islam@yahoo.com

Date received: July 1, 2020
Date received in revised form: July 29, 2020
Date accepted: August 5, 2020

Recommended citation:

> Islam, S. (2021). Security auditing tools: A comparative study. *International Journal of Computing Sciences Research*, 5(1), 407-425. doi: 10.25147/ijcsr.2017.001.1.49

Abstract

Purpose – This paper concentrates on the comparison of security auditing tools specifying password cracking tools based on different matrices. Passwords are the most popular and dominant means of access control in every authentication process. Every password is vulnerable in the virtual world; all we can do is to delay it for one to break into us. Password cracking used in two opposite intentions; either it can be used for an administrator to protect from unauthorized access and for users to recover forgotten passwords or for an intruder to break into a secure system.

Method – A great number of attacks on many systems are related to passwords. Awkwardly, the randomness and length of user-chosen passwords remain the same over time, but in contrast, hardware enhancement continuously gives intruders increasing computational power. So, password cracking has been one of the favorite vulnerable aspects for intruders to gain access to any unauthorized system. Among all available freeware password cracking tools, we choose five renowned tools based on offline and online categories.

Results – Cain and Abel is the winner in the offline category, and TCH-Hydra is the winner in the online category in their performance among the tools we have tested.

Conclusion – In this paper, the data has been collected by testing each tool several times in different systems as well as all tools in the same system based on different matrices. We have come to a knowledgeable result by comparing data among themselves. The results of the comparison will help in the adoption and usage of these tools and also promote the development and usage of security auditing tools.

Recommendations – The results of the comparison will help in the adoption and usage of these tools and also promote the development and usage of security auditing tools.

Keywords – security, cyber security, password, password cracking, security auditing tools

INTRODUCTION

Security review and security audit is a critical and essential task to perform for all organizations. It is no less than the protection of critical assets. Auditing refers to evaluating a person, organization, system, process, project, or product. Audits identify loopholes in an information security system and ensure the validity and reliability of information by assessing the current organizational structure with industry designed standards (‘IT Security Audit: Standards, Best Practices, and Tools - DNSstuff’, n.d.).

Security Auditing tools are automated tools specially designed to identify vulnerabilities in an information system that could be exploited to access privileged information (‘Auditing Tools’, n.d.). These tools perform faster and are more reliable than manual procedures. Reduced human intervention reduces the chances of errors and increases the reliability of data. These tools conduct a scan on the entire network to identify weak security areas. They help prioritize mediating efforts because the risk is categorized as high, medium, or low according to their severity of impact.

One thing is certain about security auditing tools is the power and sophistication of tools that auditors have at their disposal increase exponentially every year. Not only are the authors of these tools truly brilliant individuals (and some scary ones, too), they have also helped the security community significantly through the automation of advanced testing techniques (Jackson, 2010).

Here commences an incipient era when the Internet and incipient Network technology makes the communication more facile throughout the world. If it is about communication, then there has to be information, there is a massive amount of personal, commercial, military, and regime information on networking infrastructures worldwide. So, the Security of computers is becoming a burning question because of astute property that can be facilely compromised through the cyber world.

Modern Threats in Computer Security

Virus Threats: An indicted program that modifies the way a computer works without concern of the user. A virus replicates its copy and executes itself, which cost damage to your computer (Szor, 2005).

Spyware Threats: Any program which keeps the track of activities that are done online without the concern of a user is called spyware. The Motive behind this action can be profit or capture personal information (Good et al., 2005).

Hackers: People or a group of people who engender computer security threats and malware are known as hackers. Hackers are efficient programmers who cheat others for their benefits by entering into their network and computer systems, change, or eradicate information as a form of cyber-terrorism (Stella Adesina, 2017).

Phishing Threats: Phishers intension is to steal sensitive financial or personal information by impersonating as a reliable person, through fake email or instant messages. A computer can become a target when it relates to the Internet at the time of Network communication. Some of the most mundane attacks are Bonk, RDS_Shell, Win Nuke (Mohammad, Thabtah, & McCluskey, 2015).

Viral Web Sites: Users often got tempted by emails to visit different web sites contained with viruses or Trojans. These websites usually look like well-known websites or well-known web addresses, which are known as viral web sites. Users who visit these sites may unintentionally get affected by downloading and running viruses and Trojan (Ikinci, Holz, & Freiling, 2008).

Spyware, Advertising Trojans and Adware: Usually, without concern of a user Spyware, Advertising Trojans, and Adware are often installed with other programs. They record your behavior on the Internet, exhibit targeted ads to you. It also can download other malevolent software on to your computer. Programs or software which are downloaded free from the Internet or CD's which are given with Magazines is often included with Spyware, Adware, and Advertising Trojans. Spyware can utilize system resources and decelerate the Internet connection with the exhibit of ads, but it usually does not carry viruses. Computers can be unstable if the Spyware contains bugs (faults), but the main concern is privacy. These programs keep track of the history of user's Internet surfing and send this information to an Ad Management Centre. An Ad Management Centre reviews user searches and downloads to determine your shopping predilections. A detailed profile of that user will be build up with any concern by the Ad Management Centre, and this profile can pass on to third parties, again without any erudition (Sullivan, 2005).

Unsecured Wireless Access Points: Anyone with a wireless device can connect with the internet and can also access computers that are then connected with the network if a wireless access point is not secured (Savoor, 2012).

Bluesnarfing: The act of stealing personal data, contact information from a Bluetooth enabled device is called Bluesnarfing (Jamaluddin, Zotou, Edwards, & Coulton, 2004).

Social Engineering: Social Engineering is an art of illuming computer users to reveal his computer security or private information. It includes emotional response and trust by the target (user), which exploited by the attacker (Algarni, Xu, & Chan, 2014).

Tools Utilized in Security Susceptibility Assessment

Security susceptibility assessment tools are not only used in the intention of attack into a network but for access to sensitive data and information as well as to the targeted system.

Scanners: Scanner, a tool to gain information about a network or a specific host. This tool is developed to review the networks and report security-related information. A scanner is used in two different intentions, as a security administrator to protect systems on a network from intruders and as intruders for breaking into. This tool can be divided down into two types: network auditing implements and host-predicated auditing implements (Debar, Dacier, & Wespi, 1999).

Sniffers and Snoopers: A sniffer monitors and logs network data. Network traffic across a network is full of packets that are sent by the sender to the receiver consists of valuable information like username password. Data is transmitted without encryption in a network always is a juicy chance for intruders who have physical access to the network. Intruders can monitor the network traffic and obtain indispensable information to attack other hosts connected in the network by easily plugging in a sniffer. A snooper, also known as spyware, monitors a user’s activities by snooping on a terminal emulator session, monitoring process memory, and logging a user’s keystrokes (Stallings, 2006).

Spoofing Tools: Across a network, a data packet always contains the source address field, which can expose the source of the intruder if he sends maleficent packets. Hence, to conceal and eschew detections, the intruder uses spoofing implements to counterfeit another source address that is conventionally the address of another host or a nonexistent address. The spoofed address can be an IP address or a physical address, depending on the type of the network (‘*What is IP Spoofing? | Cloudflare*’, n.d.).

Trojan horse: A Trojan horse is defined as a maleficent, security-breaking program in a computer, which is a piece of executable code hiding in an ordinary program. When the mundane program is opened or executed, the hidden code will perform some malevolent actions silently, such as expunging critical system files. The Trojan horse is spread in a concealed way. It presents itself as a game, a web page, or a script that magnetizes people (Margaret Rouse, n.d.).

Password Crackers: A password cracker is to find a user's password. This tool is used in two opposite intentions, by intruders and system administrators for recovering lost or unknown passwords. There are three major types of cracking approaches. Intelligently guessing the password predicated on the user's information, such as user denomination, day of birth, and phone number. Dictionary attack creates an astronomically immense set of possible passwords, called a dictionary, from an accumulation of words and phrases. Both intelligent guessing and dictionary attack are astute and expeditious. If the password is arbitrarily created, these two approaches might get failed in recovering passwords. A brute force attack is a brute-force way of identifying and testing all possible passwords. Strong passwords (a combination of characters, digit, special characters (%, $, @, #,*, ^, etc.), uppercase and lower case) will customarily take a tremendous duration (Toxen, 2003).

DoS (Denial of Service) Tools: A DoS (Denial-of-Accommodation) implement is utilized by an assailant to avert legitimate users from utilizing their subscribed accommodations. DoS attacks aim at a variety of services and accomplish the objective through a variety of methods (*'What is a denial of service attack (DoS) ? - Palo Alto Networks'*, n.d.).

Stealth and Backdoor Implements: Back doors are programs cautiously installed in the target system. They are maleficent replacements of critical system programs that provide authentication and system reporting accommodations. Backdoor programs provide perpetuated and un-logged utilization of the system when being activated, conceal suspicious processes and files from the users and system administrators, and report erroneous system status to the users and system administrators (Rouse, n.d.).

Buffer Overflow: A buffer overflow tool launches attacks by inserting an oversized block of data into a program's input buffer and stack to enable an intruder to execute a piece of malicious code or destroy the memory structure. If the obscure space is a part of the framework stack, which saves the return addresses, the unremarkable return location to the location indicating the evil code may be transmuted by the overwritten part. Without the boundary checking, the intruder can compose information on the buffer and also can overwrite some obscure space in the memory (Trost, 2009).

How Password Cracking Works

In recent years, cyber-attacks on major web services like Twitter, Google, Facebook, and government websites appeared on a weekly or monthly basis. Because maximum cracking tools that are used to crack passwords are available for free. There are several ways to cracking a password or saying more specifically; there are several ways how password cracking tools works, such as dictionary attack, brute force attack, rainbow table attack.

Dictionary Attack: Dictionary attack is a common attack that is used by all the cracking tools. Its way of working is simple. There will be a .txt or .lst, which contains all the words of the dictionary or all the words possible. When tools are using this type of attack, each word is converted to hash and cross-matched against the source hash. A custom-made wordlist can be made based on the information of a very particular target. A dictionary is as good as your wordlist is. An eight-character password encodes to one of 4096 * 13-character strings. So, a dictionary of say 2,000,000 common words, names, passwords, and simple variations would amount to some 20 GB (Brogada, Sison, & Medina, 2019).

Brute force Attack: A brute force attack is cross matching all the words (hashes) possible against the hash of the source. Normally brute force attack takes too much more time than other types of attacks. It can be run for many days. But it gives more success possibilities than the other attack types (Natgunanathan, Mehmood, Xiang, Beliakov, & Yearwood, 2016).

Rainbow Table Attack: A rainbow table is a pre-computed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters. It is a practical example of space/time trade-off, using more computer processing time at the cost of less storage when calculating a hash on every attempt, or less processing time and more storage when compared to a simple lookup table with one entry per hash (H. Kumar et al., 2013).

Password Reset: Nowadays, there is a common cracking technique. The attacker somehow gains access to the target email address. Then he attempts to login at the site and tries to use the reset password option. When he used the password reset option, an email will be sent to the previously gained email address. This is how a password can be cracked using a password reset ('How Hackers Get Passwords Using These 7 Methods | SentinelOne | SentinelOne', 2019).

Overview of Password Cracking Tools

There are many password cracking tools available but among them, the popular ones are Cain & Abel, John the Ripper, Ophcrack, TCH-Hydra & Medusa ('*Password auditing – SecTools Top Network Security Tools*', n.d.). They mainly use brute force attack and dictionary attack to crack the password. But based on their functionality they are divided into two categories. They are explained here below.

Offline Password Cracking Tools

Offline password crackers do not need an active internet connection to demonstrate a cracking. PC configuration plays an important part in the cracking procedure. The higher the PC's processor and ram are, the faster the password cracker will work. The more the

PC's processor is, more number of hashes will check by the software in per second. We choose Cain & able and Ophcrack in the offline password cracker category.

Cain & Able: Cain & Abel (often abbreviated to Cain) is a password recovery tool for Microsoft Windows & created independently of Microsoft. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using a dictionary, brute-force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords, and analyzing routing protocols. The main goal is to take advantage of different hacking techniques and use them together into a program for password recovery. Cain & Abel is maintained by Massimiliano Montoro & Sean Babcock. It ranked number 1 password cracker in the Insecure.Org 2006 survey (Yazdi, 2015).

Ophcrack: Ophcrack is a free Windows password cracker based on rainbow tables. It comes with a Graphical User Interface and runs on multiple platforms. This is a new variant of Hellman's original trade-off, with better performance. It recovers 99.9% of alphanumeric passwords in seconds. Rainbow tables for LM hashes are provided for free by the developers. It is a very efficient implementation of rainbow tables done by the inventors of the method. By default, Ophcrack is bundled with tables that allow it to crack passwords no longer than 14 characters using only alphanumeric characters. Available for free download are four Windows XP tables and four Windows Vista tables (‘Ophcrack 3.3.1 & LiveCD - Free Rainbow Table Password Cracking Tool - Darknet’, n.d.).

Online Password Cracking Tools

Unlike offline crackers, online crackers need an active internet connection. Pc configuration does not have any important role unless we are using a multi-threading option. Let Assuming an attacker’s internet connection has an upload speed of 55KB/s, and each attempt is 0.5KB in size. It means the attacker’s online cracking software can make 110 attempts per second. We choose TCH-Hydra and Medusa in the offline password cracker category.

THC-TCH-Hydra: TCH-Hydra, also known as THC-hydra is a command lined based password cracker for Linux, BSD, Solaris, Mac OS X, UNIX, Windows (Cygwin). It was first developed in the year 2002. It also has a GUI version for Linux. When the remote authentication service is the target, the TCH-Hydra is often the tool of choice. It is a parallelized logon cracker. It can run a maximum of 128 tasks/children at a time. Several modules are currently supported by THC-hydra. This tool gives the researchers and security consultants the possibility to show how easy to get access to an unauthorized system. Currently, the tool is maintained by van Hauser and David Maciejak (Basta et al., 2013).

Medusa: Medusa is intended to be a speedy, massively parallel, modular, login brute-forcer. With medusa, Brute-force testing can be performed against multiple hosts, users, or passwords concurrently. Target information (host/user/password) can be specified in a variety of ways. For example, each item can be either a single entry or a file containing multiple entries. Additionally, a combination file format allows the user to refine their target listing. Each service module exists as an independent .mod file. This means that no modifications are necessary to the core application to extend the supported list of services for brute-forcing. It can perform rapid dictionary attacks against more than 30 protocols, including telnet, FTP, HTTP, HTTPS, Server Message Block (SMB), several databases, and much more. New modules are easy to add, besides that, it is flexible and very fast. The goal is to support as many services that allow remote authentication as possible('Foofus Networking Services - Medusa', n.d.). However, Zhang et al. analyzed different loud security auditing protocols and recommended that auditing mechanisms need to be designed to maintain trust and transparency within the cloud environment (Zhang, Wuwong, Li, & Zhang, 2010).

Related Works

According to Wang et al. security testing and auditing can minimize the risk and threats of a computer system (Wang, Wang, Feng, & Pan, 2016). Mohamed et al. designed and developed a security auditing tool called SAT (Security Administration Tool) and tested it on three common operating systems (Windows 95/98/NT/2000, Linux, and Solaris) to find their weakness and vulnerabilities. This tool found efficient in detecting the weakness of the systems (Mohamed, 2001). On the other hand, a rule-based security auditing tool was proposed by Moohun et al. (2006). for detecting malicious codes and software vulnerabilities. According to them, because of the limitation in the specification area, the existent detection tools are not suited to general software. They showed that the proposed tool was effective in that case (Moohun et al., 2006).

Kaur et al. mentioned in their research that Cain & Abel password recovery tool is a free and very useful for security auditing or any penetration testing of a system (Kaur & Malhotra, 2015). Much other research also found the same (Chester, 2015). On the other hand, John the Ripper tool proposes different methods to generate passwords and can crack a password with a relatively small number of gausses (Dell'Amico, Michiardi, & Roudier, 2010). However, OphCrack is a fast rainbow table-based password brute force (Graves, 2008).

According to Kakarla et al., THC-hydra is a very useful password cracking tool which can perform very fast dictionary attacks against several protocols like HTTP, HTTPS, FTP, etc. It is a fast and stable Network Login Hacking Tool which uses a dictionary or brute-force attacks to try various password and login combinations on a login page (Kakarla, Mairaj, & Javaid, 2018). Medusa is capable of testing about 2000 passwords per minute on a local system. It is useful for parallel attacks like cracking passwords of several emails at the same time. This tool is compatible with Linux, Windows, Sun OS, Mac operating systems (Kumar & Farik, 2017).

Evaluation Approach

For Offline Password Cracking Tools

For the experiment, we used two machines. One of them has the configuration of Processor: Intel(R) Core(TM) i3-2330M CPU @ 2.20GHz (4 CPUs), ~2.2GHz & Memory (RAM): 2048 MB. From now we will mention this machine with the name "Computer 1," and the other one has the configuration of Processor: Intel(R) Core(TM) 2 Duo CPU E7500 @ 2.93GHz (2 CPUs), ~2.92 GHz & Memory (RAM): 2048 MB. Again, from now, we will mention this machine with the name "Computer 2". For the experiment, we run each test 3 times in each machine for each tool.

With Cain and Able, we check the different combinations of passwords in both pc. We check the default sam file, which contains the LM & NTLM hashes of windows. We tried to crack them with a brute-force attack. Thirteen of our test cases from 27 test cases were successful. Computer 2 takes less time than Computer 1 in breaking.

There is another option of a dictionary attack to crack the hashes. As we mentioned previously, a cracking tool is as useful as the wordlist is. There is an option in Cain and Able, which changes the wordlist based on different rules like Reverse, lowercase, Uppercase, and a double pass. Setting these rules will take extra time in cracking so they can be unchecked while breaking.

We tested John, the ripper in the computer 1. John, the ripper, has different types of cracking modes. They are single crack mode, wordlist mode, and incremental model. We used both single crack mode and wordlist mode. Usually, there are no rules to set when we were using a single crack mode. But wordlist mode has rules Cain and Able. A hash type can be forced with John, the ripper. John can sort the wordlist because a shorted wordlist can make complete the cracking faster. But based on the hash type, it is preferable not to short the wordlist.

John has the unique ability to restore a previously aborted session. Not only that, the aborted session in one platform can be restored on another platform. We tested Ophcrack in computer 1. Ophcrack supports two cracking modes only. Brute force and Rainbow table attack. Ophcrack only supports 14 characters long password cracking. It does not use a powerful brute force cracking, but it is very successful with a rainbow table. The tables need to download before the cracking starts. There are several tables available for free download.

For Online Password Cracking Tools

For the experiment, we used two machines. One of them has the configuration of Processor: Again, we used our previously mentioned Computer 1 and Computer 2. For the experiment, we run each test 3 times in each machine for each tool. The reason was to minimize the effect of the Internet connection's performance on the test results and to obtain realistic measurements. The performance of the Internet varies depending on the time of day and other factors such as internet traffic, subscribed users, etc.

Data Analysis & Discussion

Data Analysis of Offline Password Cracking Tools:

The analysis of Ophcrack is given in Table 1. From the chart (Figure 1), we see that until the password is containing only the characters and numbers, it took 0.10 seconds for Ophcrack to find the correct password from the rainbow table. But from when we are using a German character and special character, the elapsed time is multiplied with almost 76, 135& 155 percent. But whatever the passwords are, it took a couple of minutes for Ophcrack to match it with the predefined list of hashes (Rainbow Table).

The chart (Figure 2) for Cain and able is showing (Table 2) a simple password which only contains a single case, numbers can be brute forced within 10 minutes. But a little complexity like both cases could take hours. Adding words with the numbers can take up to 5 - 6 hours to complete based on pc configuration. Again, adding a special character will be the password much complex, which could take 8 - 9 hours.

By analyzing the collected data and depending on different parameters, we came to a decision that Cain and Able tool are better than John the ripper and Ophcrack. Our result may be varies depending based on user requirements. Here the pie charts (Figure 3) are showing the success rate and failure rate in our case studies.

Data Analysis of Online Password Cracking Tools

We tested both TCH-Hydra and Medusa in two different circumstances. Computer 1 is connected to the network using a 150MB/s wireless router with an upload speed of average 60KB/s. And Computer 2 is connected to a network using a 300MB/s wireless router with an upload speed of average 28KB/s. Both the router speed and upload speed affected our testing. Here the speed comparison of TCH-Hydra and Medusa (Table 3) is showing for the computer 1.

In this experiment, speed data for three popular services supported by both TCH-Hydra and medusa are analyzed. The test for each module in each tool was run 3 times. And the shown value is the minimum value of each three runs. A lower value indicates better. Each tool was configured to run 1, 4, 8, and 12 task(s)/job(s) at a time (Figure 4). Both tools were tested in Computer 1 & Computer 2.

Table 1. Speed Comparison using Ophcrack in Computer 1

Passwords	Charset Used	Password Length	Time Elapsed	Cracking way	Result
Xyz	(a – z)	1 to 3	0.1 Second	Brute Force (No need to use Rainbow table)	Success
Xyzxyz	(a – z)	1 to 6	0.1 Second	Rainbow Table	Success
xyzxyz12	(a – z) + (0 - 9)	1 to 8	0.2 Seconds	Rainbow Table	Success
xyzxyz1212	(a – z) + (0 - 9)	1 to 10	0.2 Seconds	Rainbow Table	Success
xyzxyz121212	(a – z) + (0 - 9)	1 to 12	0.9 Seconds	Rainbow Table	Success
xyzxyz12121212	(a – z) + (0 - 9)	1 to 14	0.7 Seconds	Rainbow Table	Success
äxyz%	German + (a – z)	1 to 5	1 m 16 Seconds	Rainbow Table	Success
xäyz&*	German + (a – z) + Special Character	1 to 7	2 m 16 Seconds	Rainbow Table	Success
äxyz #@!	German + (a – z) + Special Character	1 to 8	2 m 35 Seconds	Rainbow Table	Success
123xyz ä^&*	German + (0-9) + (a – z) + Special Character	1 to 11	Unknown	Rainbow Table	Unknown

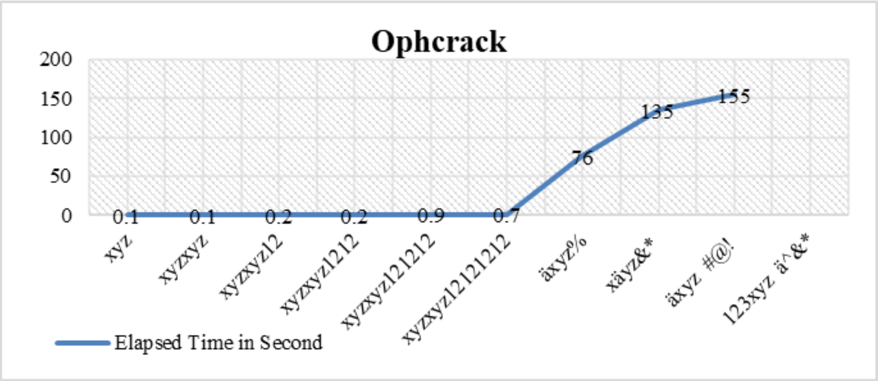

Figure 1. Speed comparison different passwords using Ophcrack for computer 1

Table 2. Speed Comparison using Cain and able in both Computer 1 & 2

Passwords	Charset Used	Password Length	Computer 1		Computer 2	
xyz	(A – Z)	1 to 6	0.88 minute	Fail	0.56 minute	Fail
xyz	(A – Z) + (0 - 9)	1 to 6	1.23 minute	Fail	0.76 minute	Fail
xyz	(A – Z) + (0 - 9) + Special Character	1 to 6	42.5 minute	Fail	27.36 minute	Fail
xyz	(0 - 9)	1 to 6	0.0 minute	Fail	0.0 minute	Fail
xyz	(a – z)	1 to 6	0.1 second	Success	0.1 second	Success
xyz	(a – z) + (0 - 9)	1 to 6	0.1 second	Success	0.1 second	Success
xyz	(a – z) + (0 - 9) + Special Character	1 to 6	0.1 second	Success	0.1 second	Success
xyz	(A – Z) + (a – z) + (0 – 9)	1 to 6	0.1 second	Success	0.1 second	Success
xyz	(A – Z) + (a - z) +(0 - 9) + Special Character	1 to 6	0.1 second	Success	0.1 second	Success
xyzxyz	(A – Z)	1 to 6	0.9 minute	Fail	0.54 minute	Fail
xyzxyz	(A – Z) + (0 - 9)	1 to 6	6.33 minute	Fail	3.8 minute	Fail
xyzxyz	(A – Z) + (0 - 9) + Special Character	1 to 6	45.31 minute	Fail	27.9 minute	Fail
xyzxyz	(0 - 9)	1 to 6	0.0 minute	Fail	0.0 minute	Fail
xyzxyz	(a – z)	1 to 6	0.88 minute	Success	0.54 minute	Success
xyzxyz	(a – z) + (0 - 9)	1 to 6	6.32 minute	Success	3.87 minute	Success
xyzxyz	(a – z) + (0 - 9) + Special Character	1 to 6	44.08 minute	Success	28.2 minute	Success
xyzxyz	(A – Z) + (a – z) + (0 – 9)	1 to 6	2.28 hours	Success	1.68 hours	Success
xyzxyz	(A – Z) + (a - z) +(0 - 9) + Special Character	1 to 6	8.88 hours	Success	5.66 hours	Success
xyzxyz12	(A – Z)	1 to 8	9.51 hours	Fail	6.26 hours	Fail
xyzxyz12	(A – Z) + (0 - 9)	1 to 8	5.29 days (est)	Fail	3.43 days (est)	Fail
xyzxyz12	(A – Z) + (0 - 9) + Special Character	1 to 8	72.52 days (est)	Fail	47.1 days (est)	Fail
xyzxyz12	(0 - 9)	1 to 8	0.0 minutes	Fail	0.0 minutes	Fail
xyzxyz12	(a – z)	1 to 8	10.02 hours	Fail	6.53 hours	Fail
xyzxyz12	(a – z) + (0 - 9)	1 to 8	5.4 days (est)	Success	3.63 days (est)	Success
xyzxyz12	(a – z) + (0 - 9) + Special Character	1 to 8	74.49 day (est)	Success	49.87 days (est)	Success
xyzxyz12	(A – Z) + (a – z) + (0 – 9)	1 to 8	1.18 years (est)	Success	266.7 days (est)	Success
xyzxyz12	(A – Z) + (a - z) +(0 - 9) + Special Character	1 to 8	5.63 years (est)	Success	3.71 years (est)	Success

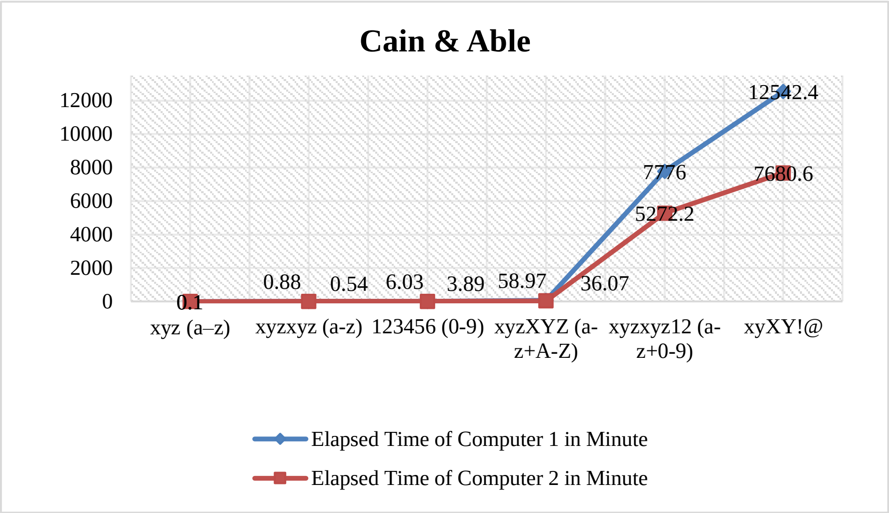

Figure 2. Speed comparison of Cain& Able for both computer 1 & 2

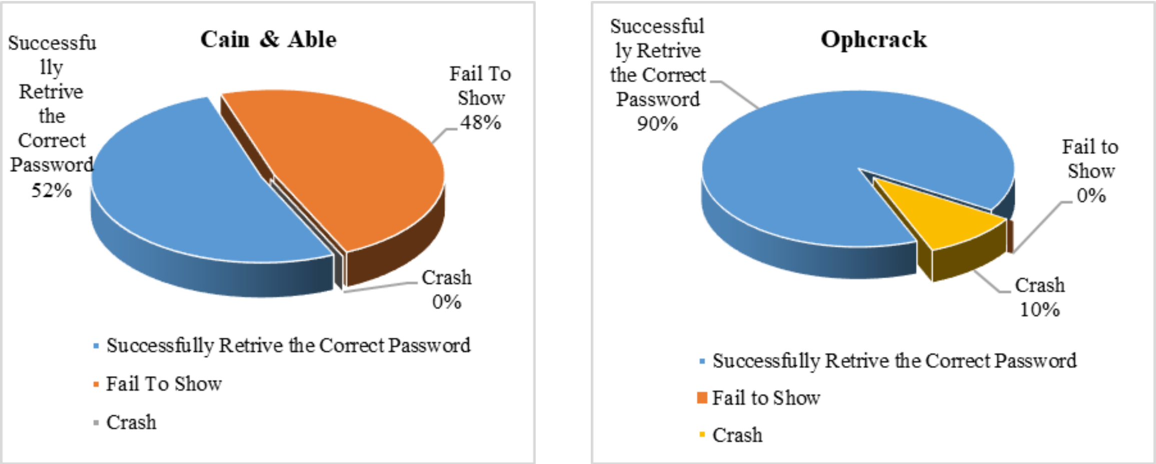

Figure 3. Success and failure rate in our case studies

Table 3: Speed Test Comparison of TCH-Hydra & Medusa Based on HTTP Module

Module	**Password List Entries**	**Valid Password**	**Target**	**Task(s)**	**TCH-Hydra**		**Medusa**	
					PC 1	**PC 2**	**PC 1**	**PC 2**
HTTP Module	3000 Entries	at # 3000	192.168.1.1	1 Task	48s	28s	47s	29s
				4 Task	47s	27s	47s	26s
				8 Task	47s	27s	47s	25s
				12 Task	47s	26s	47s	25s

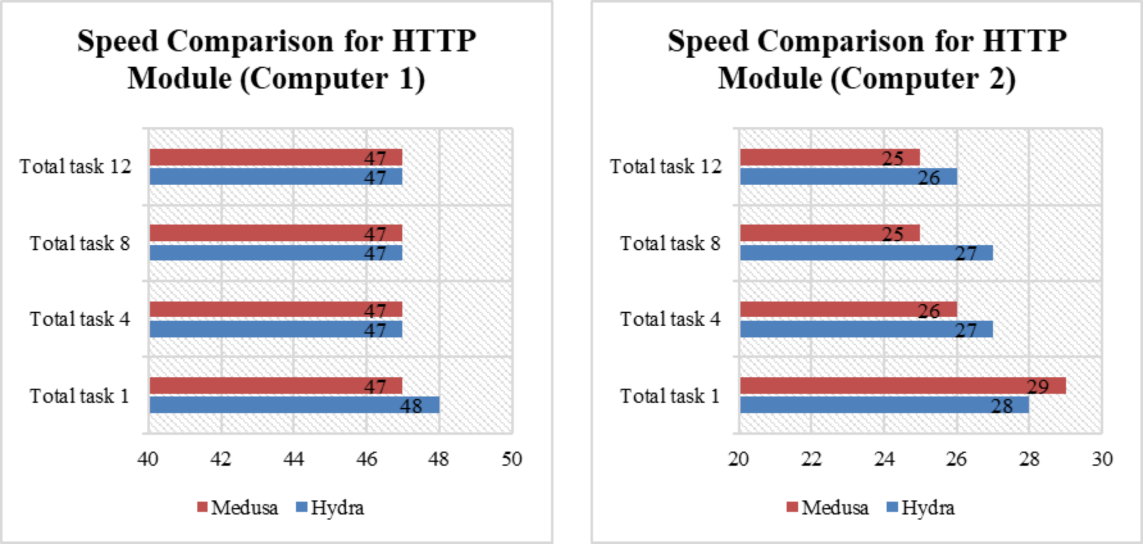

Figure 4. Speed Comparison of TCH-Hydra & Medusa for HTTP Module

Here in Table 4 we see that for the FTP module TCH-Hydra and Medusa are taking the almost same time. Even they are taking the same time when multiple tasks are running. This is because total testing executed locally where only the speed of different routers installed with computer 1 & 2 matters. But even if they are almost the same, Medusa is few seconds ahead of TCH-Hydra for each 1, 4, 8, and 12 tasks (Figure 5). Again, for the FTP module, TCH-Hydra is ahead of Medusa when there is only one task. But Medusa gives a better result than TCH-Hydra when the task number is 8 and 12 (Figure 6).

Table 4: Speed Test Comparison of TCH-Hydra & Medusa Based on FTP Module

Module	Password List Entries	Valid Password	Target	Task(s)	TCH-Hydra		Medusa	
					PC 1	PC 2	PC 1	PC 2
FTP Module	16 Entries	at # 15	31.170.166.140	1 Task	1.14m	1.32m	1.21m	1.14m
				4 Task	19s	26s	The 20s	28s
				8 Task	9s	11s	8s	9s
				12 Task	7s	8s	6s	9s

With the SMTP module (Table 5), Medusa may be won the race with 1 task, but TCH-Hydra was taking less time with multiple children to complete the job. So, based on the collected data and depending on different parameters we came to a decision that TCH-Hydra is better than Medusa. Our result may be varies depending based on user requirements. Here the pie charts (Figure 7) are showing the success rate and failure rate in our case studies.

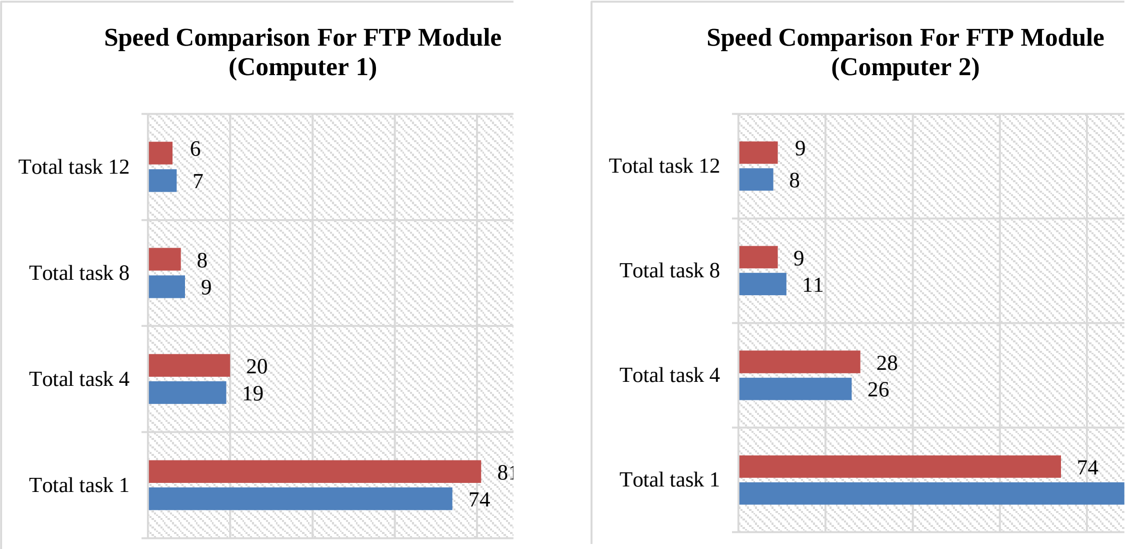

Figure 5. Speed Comparison of TCH-Hydra & Medusa for FTP Module

Table 5: Speed Test Comparison of TCH-Hydra & Medusa Based on SMTP Module

Module	**Password List Entries**	**Valid Password**	**Target**	**Task(s)**	**TCH-Hydra**		**Medusa**	
					PC 1	PC 2	PC 1	PC 2
SMTP Module	500 Entries	at # 100	smtp.gmail.com	1 Task	2.39 m	3.7 m	2.22 m	2.45 m
				4 Task	40s	45s	48s	54s
				8 Task	34s	37s	36s	43s
				12 Task	22s	29s	26s	29s

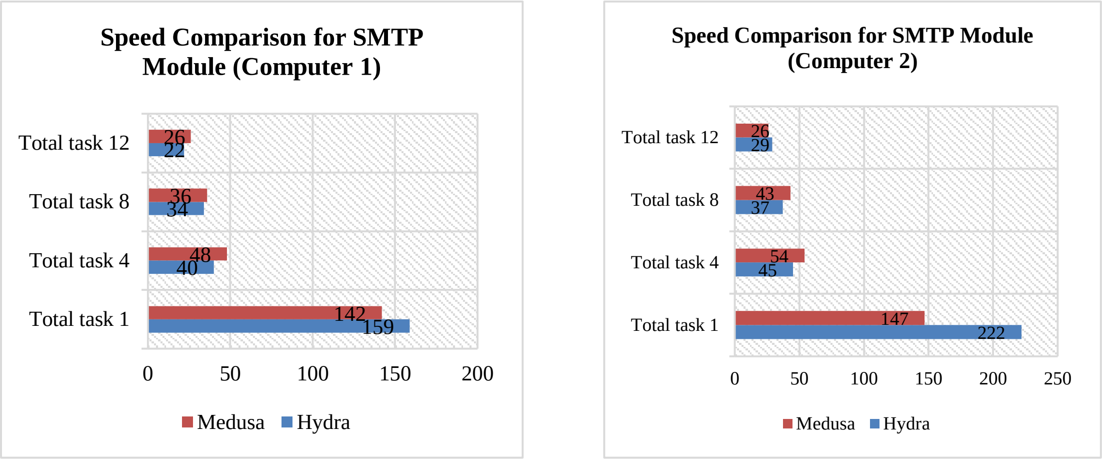

Figure 6. Speed Comparison of TCH-Hydra & Medusa for SMTP Module

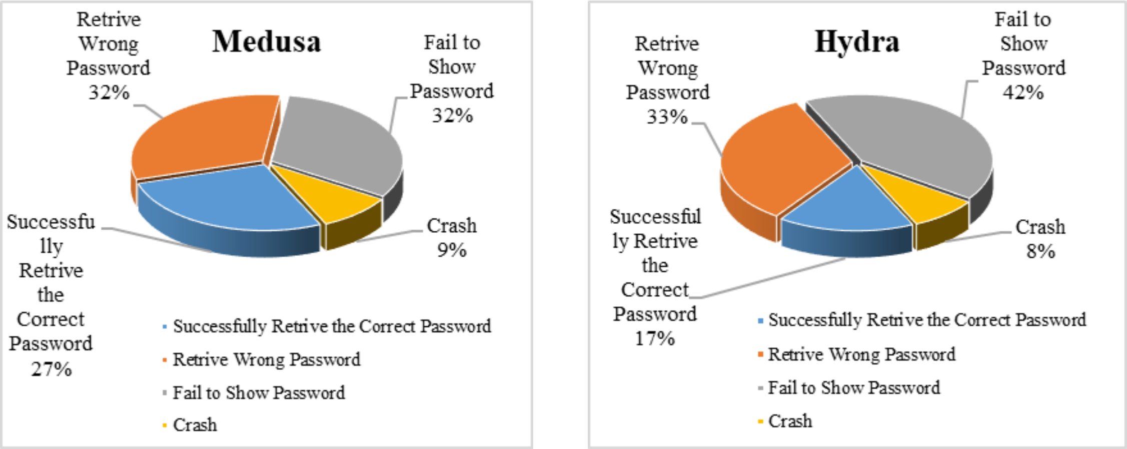

Figure 7. Success and failure rate in our case studies with TCH-Hydra

Conclusion

Password is taken as a dominant means of access control in every authentication process though there are other options are available now like face detection, voice recognition, and fingerprint matching are used for the sake of security. As far as the security of a system is concerned, a large number of attacks on many systems are related to the passwords. Awkwardly, the randomness and length of user-chosen passwords remain the same over time, and passwords are kept insecurely in the operating systems, but in contrast, hardware enhancement continuously gives intruders increasing computational power. So, password cracking has been one of the favorite vulnerable aspects for intruders to gain access to any unauthorized system. We choose five renowned tools based on the offline and online categories, which are used in password cracking.

It has been shown here that the tools have been used and which one of the attack types supported by the tools we tested. Then, some test cases have been selected based on requirements and test the tools at least three times for each test case. Later on, from the collected data, a speed comparison has been demonstrated among the tools.

Based on some prefixed parameters, five tools have been compared in two categories. Since the offline cracking tools do not share the same type of attacking mode, so they were not compared among themselves. But a speed test was demonstrated for different password combinations in the different computers for the same offline cracking tool. Again, for the online cracking tools as they share the same attack mode. So, the speed comparison was presented for both tools in the same computer and each tool in two different computers. This speed test analysis will help to identify the better tool among all the tools in both categories. Cain and able is the winner in the offline category, and TCH-Hydra is the winner in the online category in their performance among the tools we have tested. The results of the comparison will help in the adoption and usage of these tools and promote the development and usage of security auditing tools.

REFERENCES

Algarni, A., Xu, Y., & Chan, T. (2014). Social engineering in social networking sites: The art of impersonation. In *Proceedings - 2014 IEEE International Conference on Services Computing, SCC 2014* (pp. 797–804). Institute of Electrical and Electronics Engineers Inc. Retrieved from https://doi.org/10.1109/SCC.2014.108

Auditing Tools. (n.d.). Retrieved 28 July 2020, from http://www.secure-bytes.com/auditing-tools.php

Basta, A., Basta, N., Brown, M., & CISSP, C. (2013). *Computer security and penetration testing*. Cengage Learning.

Brogada, M. A. D., Sison, A. M., & Medina, R. P. (2019). Cryptanalysis on the head and tail technique for hashing passwords. In *Proceeding - 2019 IEEE 7th Conference on Systems, Process, and Control, ICSPC 2019* (pp. 137–142). Institute of Electrical and Electronics Engineers Inc. Retrieved from https://doi.org/10.1109/ICSPC47137.2019.9068043

Chester, J. (2015). Analysis of Password Cracking Methods & Applications. *Williams Honors College, Honors Research Projects*. Retrieved 29 July 2020 from https://ideaexchange.uakron.edu/honors_research_projects/7

Debar, H., Dacier, M., & Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems. *Computer Networks*, 31(8), 805–822. Retrieved from https://doi.org/10.1016/S1389-1286(98)00017-6

Dell'Amico, M., Michiardi, P., & Roudier, Y. (2010). Password strength: An empirical analysis. In *Proceedings - IEEE INFOCOM*. Retrieved from https://doi.org/10.1109/INFCOM.2010.5461951

Foofus Networking Services - Medusa. (n.d.). Retrieved 29 July 2020, from http://foofus.net/goons/jmk/medusa/medusa.html

Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D., & Konstan, J. (2005). Stopping spyware at the gate: A user study of privacy, notice, and spyware. In *ACM International Conference Proceeding Series* (Vol. 93, pp. 43–52). New York, New York, USA: ACM Press. Retrieved 28 July 2020 from https://doi.org/10.1145/1073001.1073006

Graves, R. E. (2008). *High-performance password cracking by implementing rainbow tables on nVidia graphics cards (IseCrack)*. *Graduate Theses and Dissertations*. Digital Repository @ Iowa State University, Ames. Retrieved 29 July 2020 from https://doi.org/10.31274/etd-180810-2056

How Hackers Get Passwords Using These 7 Methods | SentinelOne | SentinelOne. (2019). Retrieved 28 July 2020, from https://www.sentinelone.com/blog/7-ways-hackers-steal-your-passwords/

Ikinci, A., Holz, T., & Freiling, F. (2008). Monkey-Spider: Detecting Malicious Websites with Low-Interaction Honeyclients. In A. Alkassar & J. Siekmann (Eds.), *SICHERHEIT 2008 – Sicherheit, Schutz und Zuverlässigkeit. Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)* (pp. 407–421). Bonn: Gesellschaft für Informatik e. V.

IT Security Audit: Standards, Best Practices, and Tools - DNSstuff. (n.d.). Retrieved 25 July 2020, from https://www.dnsstuff.com/it-security-audit

Jamaluddin, J., Zotou, N., Edwards, R., & Coulton, P. (2004). Mobile phone vulnerabilities: A new generation of malware. In *2004 IEEE International Symposium on Consumer Electronics - Proceedings* (pp. 199–202). Retrieved from https://doi.org/10.1109/isce.2004.1375935

John the Ripper password cracker. (n.d.). Retrieved 28 July 2020, from https://www.openwall.com/john/

Kakarla, T., Mairaj, A., & Javaid, A. Y. (2018). A Real-World Password Cracking Demonstration

Using Open Source Tools for Instructional Use. In *IEEE International Conference on Electro Information Technology* (Vol. 2018-May, pp. 387–391). IEEE Computer Society. Retrieved from https://doi.org/10.1109/EIT.2018.8500257

Kaur, G., & Malhotra, J. (2015). An Integrated Approach to ARP Poisoning and its Mitigation using Empirical Paradigm. *International Journal of Future Generation Communication and Networking*, 8(5), 51–60. Retrieved 29 July 2020 from https://doi.org/10.14257/ijfgcn.2015.8.5.05

Kumar, H., Kumar, S., Joseph, R., Kumar, D., Shrinarayan Singh, S. K., Kumar, P., & Kumarr, H. (2013). Rainbow table to crack password using the MD5 hashing algorithm. In *2013 IEEE Conference on Information and Communication Technologies, ICT 2013* (pp. 433–439). Retrieved from https://doi.org/10.1109/CICT.2013.6558135

Kumar, J., & Farik, M. (2017). Cracking Advanced Encryption Standard-A Review. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, 6, 7. Retrieved 29 July 2020 from www.ijstr.org

Margaret Rouse. (n.d.). What is a Trojan Horse? Definition from WhatIs.com. Retrieved 28 July 2020, from https://searchsecurity.techtarget.com/definition/Trojan-horse

Mohamed, A. B. M. (2001). An effective modified security auditing tool (SAT). In *Proceedings of the International Conference on Information Technology Interfaces, ITI* (pp. 37–41). The University of Zagreb. Retrieved from https://doi.org/10.1109/ITI.2001.937994

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, 17, 1–24. doi: https://doi.org/10.1016/j.cosrev.2015.04.001

Moohun, L., Sunghoon, C., Changbok, J., Heeyong, P., & Euiin, C. (2006). A rule-based security auditing tool for software vulnerability detection. In *Proceedings - 2006 International Conference on Hybrid Information Technology, ICHIT 2006* (Vol. 2, pp. 505–512). Retrieved from https://doi.org/10.1109/ICHIT.2006.253653

Natgunanathan, I., Mehmood, A., Xiang, Y., Beliakov, G., & Yearwood, J. (2016). Protection of Privacy in Biometric Data. *IEEE Access*, 4, 880–892. Retrieved from https://doi.org/10.1109/ACCESS.2016.2535120

Ophcrack 3.3.1 & LiveCD - Free Rainbow Table Password Cracking Tool - Darknet. (n.d.). *Https://Www.Darknet.Org.Uk/*. Retrieved 28 July 2020 from https://www.darknet.org.uk/2011/03/ophcrack-3-3-1-livecd-free-rainbow-table-password-cracking-tool/

Password auditing – SecTools Top Network Security Tools. (n.d.). Retrieved 28 July 2020, from https://sectools.org/tag/pass-audit/

Rouse, M. (n.d.). What is backdoor (computing)? - Definition from WhatIs.com. Retrieved 28 July 2020, from https://searchsecurity.techtarget.com/definition/back-door

Savoor, R. (2012). Devices and methods for secure internet transactions. Google Patents.

Jackson, C.(2010). *Network security auditing tools and techniques*. Retrieved 28 July 2020, from https://www.ciscopress.com/articles/article.asp?p=1606900&seqNum=5

Stallings, W. (2006). *Cryptography and network security, 4/E*. Pearson Education India.

Stella Adesina, O. (2017). Cybercrime and poverty in Nigeria. *Canadian Social Science*, 13(4), 19–29. Retrieved 28 July 2020 from https://doi.org/10.3968/9394

Sullivan, D. (2005). *The definitive guide to controlling malware, spyware, phishing, and spam*. Realtimepublishers. com.

Szor, P. (2005). *The Art of Computer Virus Research and Defense: ART COMP VIRUS RES DEFENSE _p1*. Pearson Education.

Toxen, B. (2003). *Real-world Linux security: intrusion prevention, detection, and recovery*. Prentice-

Hall Professional.

Trost, R. (2009). *Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century: Prevention and Detection for the Twenty-First Century*. Pearson Education.

Wang, S.-L., Wang, J., Feng, C., & Pan, Z.-P. (2016). Wireless Network Penetration Testing and Security Auditing. *ITM Web of Conferences*, 7, 03001. Retrieved 29 July 2020 from https://doi.org/10.1051/03001

What is a denial of service attack (DoS) ? - Palo Alto Networks. (n.d.). Retrieved 28 July 2020, from https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

What is IP Spoofing? | Cloudflare. (n.d.). Retrieved 28 July 2020, from https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/

Yazdi, S. H. (2015). *Probabilistic Context-Free Grammar Based Password Cracking: Attack, Defense, and Applications*. Retrieved 28 July 2020 from https://diginole.lib.fsu.edu/islandora/object/fsu%3A253086/

Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010). Information security risk management framework for the cloud computing environments. In *Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, ScalCom-2010* (pp. 1328–1334). Retrieved from https://doi.org/10.1109/CIT.2010.501