Millennial Psychology Towards Hacking Activities

Nor Azlina Abd Rahman
Forensic and Cyber Security Reseach Centre
Asia Pacific University of Technology & Innovation
Bukit Jalil, Kuala Lumpur, Malaysia
nor_azlina@apu.edu.my

Ibiwani Alisa Hussain
School of Business
Asia Pacific University of Technology & Innovation
Bukit Jalil, Kuala Lumpur, Malaysia
dr.ibiwani@apu.edu.my

Noris Ismail
School of Technology
Asia Pacific University of Technology & Innovation
Bukit Jalil, Kuala Lumpur, Malaysia
noris.ismail@apu.edu.my

Hains Jojo
School of Technology
Asia Pacific University of Technology & Innovation
Bukit Jalil, Kuala Lumpur, Malaysia
TP052181@mail.apu.edu.my

Yusra Khan
School of Technology
Asia Pacific University of Technology & Innovation
Bukit Jalil, Kuala Lumpur, Malaysia
yus.khan118@gmail.com

***Abstract*— Hacking competition has becoming popular among the teenagers especially universities students nowadays. In Malaysia there are many companies and universities that organizing the hacking competition such as F-Secure, KPMG, CyberSecurity Malaysia, Asia Pacific University, UiTM, UniKl and many others. Besides that, there are also many platforms that are available for those who are interested with penetration testing or hacking activities such as Hack the Box (HTB), picoctf, Tryhackme and many others. The facilities that available together with the individual interest has attract many people not only teenagers but also school students and adult to participate in hacking competition. Most people participating in hacking competition due to many reasons such as to gain money, sharpen the skills and sometimes people would like to try the new things or skills. This paper is focusing on the current trend of attacks, analysing the target group of people in terms of their behavior, psychology, and interest towards hacking activities. Questionnaires were prepared that focusing on demography, psychology based on extrinsic and intrinsic factors and hacking experiences questions. Based on the analysis the result would be on influence and psychology impact of the millennial towards hacking activities.**

Keywords*— *Millennial, psychology, hacking activities, attack

I. TRENDS OF CYBER ATTACKS

In today's age of advanced technological development, with exceptional progress, comes exceptional obstacles. Cyber-attacks are a prevalent and growing concern to organisations and businesses worldwide. It was found that Hackers attack every 39 seconds, on average 2,244 times a day (Sobers, 2020). With their incline, it is noticed that cyber-attacks fall into a particular trend that shifts and changes based on several different factors.

This is considered the biggest threat to cyber security as 98% of actual attacks are dependent on some form of social engineering where businesses are concerned, this is a serious threat as Internal Attacks are extremely difficult to detect and prevent. For data breaches, it has been found that 68% of the successful attacks involve internal sources (Purplesec, 2020).

One of the most popular forms of social engineering attacks is Phishing. The occurrence of these attacks is continuing to rise, and 56% of IT decision makers confirm that targeted phishing attacks are their top threat to security. This can be attributed to the fact that it depends on unaware employees from the organisation to give up some information, and this happens very often. 76% of organisations believe that their largest threat to security is carelessness of their own employees and users and falling into phishing or ransomware attacks.

This kind of attack ties in well with Phishing since 92% of malware is delivered by email. Malware infections have been on the rise for the past 10 years, with mobile malwares being more common, and 98% of mobile malware targeting Android devices. Malware poses as a more malicious type of software; this form of cyber-attack is one of the most popular kinds of attacks and certainly the costliest. This is the main type of malware used, and the number of attacks had grown in 2018 by 350% and are estimated to cost $6 trillion annually by 2021. Ransomware attacks focus on businesses with sensitive data or internet connected activities that can be ransomed (Purplesec, 2020).

With the increase in the number of 'smart' devices or IOT devices, there is the potential of an attack, since the security features installed within the devices is not very robust. According to NETSCOUT's Threat Intelligence Report it only takes 5 minutes of being connected to the internet for an IoT device to be attacked. They measured that the amount of attack traffic for IoT related attacks has increased to more than 2.9 billion.(Netscout.com., 2020).

DDoS attacks have also been growing, with a clear rise in the number of DDoS attacks between 2018 and 2019, along with their duration. Although DDoS attacks may not be the most popular cyber-attack, they certainly have a considerable impact on companies and cause millions of dollars lost in revenue. It was found that denial of service (DoS) attacks cost an average of $129,450 annually in 2017. (Packt, 2019).

In the current atmosphere the world is facing, there are exceptions to the trend, as the Covid-19 pandemic facilitates hackers and attackers to take advantage of any vulnerabilities or oversights of organisations. WHO (World Health Organisation) has seen a tremendous incline in the number of cyber-attacks directed to their organisation, including data breaches and also phishing attacks where hackers steal money by claiming to be from a legitimate WHO fund for Covid-19 (Brewster, 2020).

These include several forms of attacks like SQL injection, cross site scripting, etc. and are a common occurrence because of the many loopholes in websites including easy authorisation. It was found that 82 percent of vulnerabilities were in application code, displaying the likely sources of attacks.

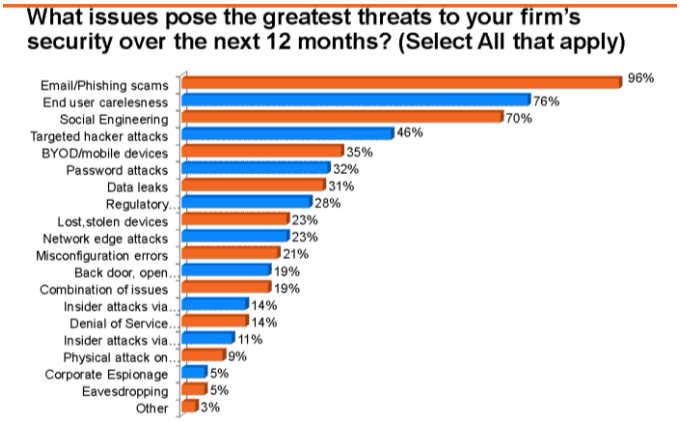

Fig. 1. Security Threats and Trends report 2019 (KnowBe4, 2019)

Fig 1. displays the most common vectors of cyber-attack that businesses fear. It can be noted that social engineering attacks surpass all other attacks in their abundance. Malware attacks can be linked to different consequences mentioned such as targeted hacker attacks and data leaks. Web-based attacks too can be attributed with vernacular mentioned like Denial of Service, and backdoors. Based on the elements mentioned before, some of the common attacks present here include Social Engineering, Malware, and DoS. Some of the other categories from the graph in Fig 1. like password attacks, backdoor, and misconfiguration errors can be directly related to attributes of another attack gaining popularity, which is IoT based attacks.

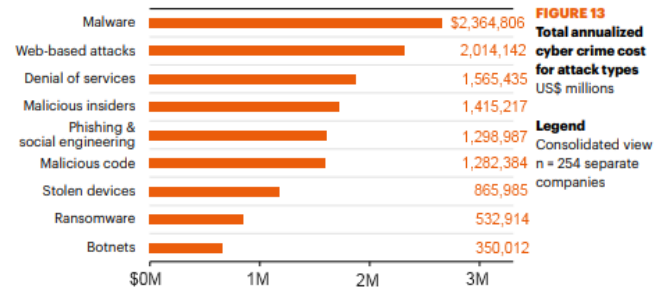

Fig. 2. Cost of cybersecurity attacks (Packt, 2019)

Fig 2. represents a more comprehensive look on the impact of cyber-attacks on financial condition of companies. Malware exceeds the rest due to the more malicious incidents involving high downtime. The attack types can be an insight into the most common forms of cyber-attacks. Other attacks mentioned here that relate to some of the most common attacks are Web-based attacks, DoS attacks, ransomware, and Social Engineering. These attacks can be seen as both the most common, and some of the costliest attacks.

II. LITERATURE REVIEW ON THE MOST COMMON ATTACK

Based on the mentioned attacks in the cyber world, there are a few areas that are more prevalent today and have been discussed in detail below. It should be noted that the trends of attacks are directly related to advancements in the cyber world, and there exists a difference between the most common attacks today as compared to the most impactful. Today, the most common attacks worldwide include social engineering, malware attacks and web-based attacks.

A. Social Engineering Attacks

Cyber-attacks today have developed over the years and social engineering has remained as the most prevalent and versatile form of manipulation. Social engineering has been defined as any action that involves influencing another person to do something that they may otherwise not have done. Although there is no technical complexity to this form of attack, its impact and its reach in organisations is undeniable (KnowBe4, 2019). Human error is a very difficult factor to control, and organizations suffer major consequences from employee mistakes involving being manipulated. For this manipulation to enter the cyber world, it is conducted in several different ways:

Phishing is the most common form of social engineering, and the most dangerous. It involves targeting a person through phone, email, or text message, and impersonating some higher authority or legitimate organisation to convince the target to release sensitive data like credentials, financial information and more. The first quarter of 2020 has seen a surge in phishing and website scams which can be attributed to the start of the Covid-19 pandemic. Of the 854,441 confirmed cases of phishing and counterfeit pages and 4M suspicious pages detected, 30% of these were related to Covid-19. (Purplesec, 2020).

SMiShing is an offspring of phishing which involves the same process except it is done over text messages. This form of attack has seen an upward trend since the spread of the current pandemic in the world today. There are many reports of people receiving messages from sources claiming to be governments or medical bodies and convincing the target of releasing information or making some payment. An example of this can be seen in the following SMS where the attacker is impersonating the UK Government. (Brewster, 2020).

Fig. 3. Spoofed SMS impersonating UK gov(Brewster, 2020)

Vishing is also another version of Phishing where the perpetrator makes his move over a call of some sort, hence the name voice phishing. It has been on a rise over the past years as it is easy, cheap, and often successful. It is also hard to trace since spoofed numbers are often used from outside the country.

Another common form of social engineering is Impersonation, and this is possibly one of the highest risk-high gain actions of manipulation. It is defined as the act of pretending to be another person, and in the case of cyber-attacks, gaining some valuable access or information from

doing so. With the spread of the current pandemic there have been many scams related to the virus in some way. One of the focuses is medical scams, where several websites were claiming to cure the virus, or spreading misinformation. There was also an increase in the number of domain registrations that contained things like 'stimulus checks and more websites claiming to give loans to small businesses (Help Net Security, 2020).

B. *Malware Attacks*

Researchers discussed the various threats to computer systems and its prevention. The areas covered are part of a category known as malware, which is described as any software that is made with malicious purpose and is in the form of any file or program that is harmful to the user. Under this category exist a few different types including viruses, trojans, spyware, and worms (Tasril et al., 2017).

The computer virus is one of the oldest forms of any malicious software and can be described as a program that modifies other computer programs and inserts its own code to replicate itself when executed. Trojans are more dangerous form of malware that are capable of malicious activity while misleading the user of its true intent. It is a client-server type of program that is remotely controlled, all without the knowledge of the user. This program allows the attacker to assume full or partial control of the system, and steal information or carry out a crime. Worms are another type of malware that are of less danger but can still cause a considerable amount of damage. It is a standalone malware that can replicate itself and spreading to other computers over a network connection. Worms will enter a computer's registry and enable a script to multiply itself, all without the knowledge of the user.

Another variation of malware is ransomware. This malware is one where the attacker will threaten to publish or block access to some sensitive data until a ransom is paid. Ransomware is gaining popularity in the last few years and although the occurrences are fewer compared to phishing, the impact and cost is higher since the ransom usually outlines a healthy sum of money. The method of attack is carried out either by locking access to the user's system (locker ransomware), or a more advanced method that involves encrypting the users' files and demanding a ransom for their decryption (crypto ransomware) (Karaffa, 2017).

An example of this case occurring in a real-life setting can be seen in the WannaCry incident. On May 12th, 2017, a cyber-attack occurred that affected 200,000 computers across 100 countries, with high-stake organisations affected like the NHS in the UK. The target machine was computers running Windows, after which the victims' files were held hostage, and a fee was demanded for the files in the form of bitcoin (Nao.org.uk., 2020).

Ransomware infection along with other malwares causes a serious amount of damage mostly to organisations. As these malwares are targeting larger organisations, there is an incline in the monetary loss. The ransom fees demanded are increasing and the organisations targeted have become more high-profile. The largest impact of these is the cost associated with downtime, which includes both businesses that have their systems compromised, or those companies that shut down their systems as a preemptive measure to protect them from an ongoing cyber-attack. This leads to many consequences from a business aspect.

C. *Web Based Attacks*

Based on research by Lomte R. M. and Bhura S. A., of all cyber-attacks, around 80% are on the application layer, and 90% of applications are vulnerable to these kinds of attacks. Web based attacks all those that target the way one uses an operating system or application and are usually more difficult to prevent (Lomte & Bhura, 2013). OWASP 2020 commits to providing a guideline for application development to prevent against some common application attacks. Some attacks included in these are SQL injection, cross site scripting, broken authentication, sensitive data exposure, XEE, broken access control, security misconfiguration, insecure deserialisation and insufficient logging and monitoring (Owasp.org., 2020).

SQL Injection or SQLi, is an injection attack that allows one to execute malicious sql statements which are designed to control the database server behind some web application and bypass application security measures. It can lead to many consequences such as unauthorised access to personal data or intellectual property. Injection is still the most common application attack according to OWASP.

Another malicious web-based attack is cross site scripting (XSS) which enables attackers to inject some script from the client side to an application that is viewed by others. This will lead to the webpage loading with user-supplied data which may create HTML or Javascript files. This leads to the attacker being capable of executing malicious scripts in the user's browser. This usually occurs due to the lack of proper validation or escapes.

III. ANALYSIS ON TARGETED MILLENNIAL

There are any many reasons of people involvement in attack activities. Some of the reasons due to financial gain, hacktivism, intellectual challenge, and many other reasons. A survey had been conducted where the scope of the area is around Klang valley area with 100 respondents. The purpose of the study is to identify the "Millennial Psychology" towards Hacking Activities.

A. *Demography*

100 respondents with different age background ranging from 16 to above 25 years old have participated in the survey as shown in Fig 4.

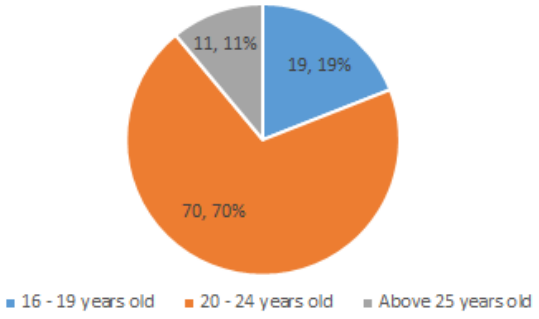

Fig. 4. Age range of the participants

70% of them are from the middle age group that is between 20 to 24 years old. This age of group are those who are creative and like to explore new things. This can be supported with

several top 10 teen hackers such as Kevin Mitnick who hacked Digital Equipment Corporation's (DEC) network and made copies of their software in 1989, Adrian Lamo who used an unprotected content management tool at Yahoo to modify a Reuters article in 2001(Kaspersky, 2020).

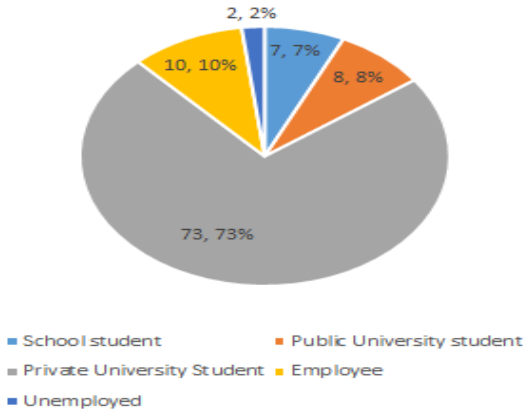

Fig. 5. Academic Background

Based on Fig 5., 73% of respondents are private university students, followed by 10% employee, 8% public university students, 7% school students and 2% unemployed. As in general looks like students are the most who involved in hacking activities.

These are the group of people that have enough time to explore in this area maybe due to their interest, more spare time and this area could be related to their course or academic curriculum.

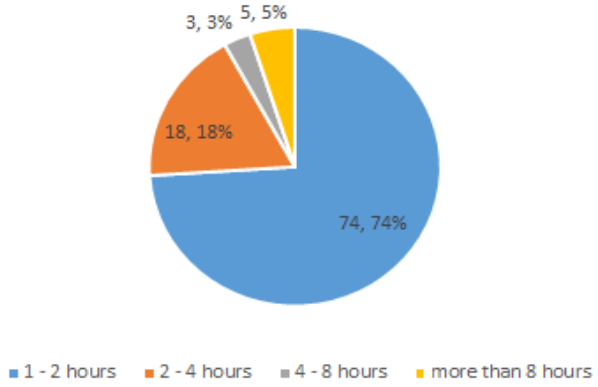

Fig. 6. Time Spent for hacking activities

Based on data tabulated in Fig 6. shows that majority of the participant which is 74% spent around 1-2 hours in hacking activities, followed by 18% spent around 2-5 hours, 5% spent 4-8 hours and 3% of participants spent more than 8 hours in hacking activities. Those who are more than 8 hours spent in hacking activities showed that they are very passion in this area. This group of millennials are also those who were actively participated in hacking competition.

B. Hacking Background

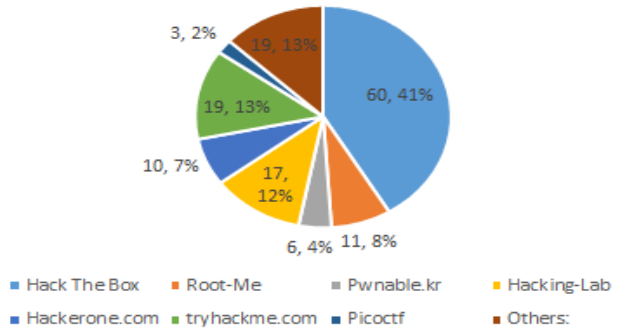

Fig. 7. Hacking and penetration testing Platform

Based on Fig 7., the findings on the platform used by the targeted group to practice their hacking skills have shown that 41% of the respondents are using Hack the Box, 13% are using Tryhackme and 12% are using Hacking-Lab websites. These websites provide platforms for the registered users to learn and to test their hacking skills by providing virtual or live machines and challenges. Besides educating and training, these websites create platforms for its users to communicate and share knowledge among themselves. There are also amusing, game-oriented platforms for both web and mobile applications in which users can explore. Some of the platforms that are also mentioned are Root-Me that is 8%, Hackerone.com – 7%, Pwnable.kr – 4%, Picoctf – 2% and others – 13%.

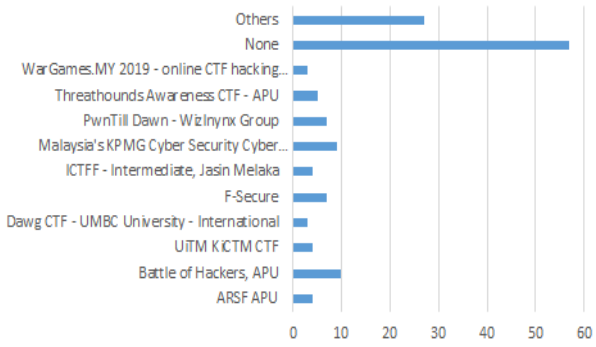

Fig. 8. Participants experiences in hacking competition

From the statistics gathered (Fig 8.) also have shown that 59% of the respondents who have involved in this hacking activities, must have at least participated or exposed to at least one hacking competition to test their knowledge and skills in this area. Those who have participated in the hacking competition can be divided into two categories that are online and on-site competition.

81% of the respondents have participated in an on-site competition that is organized by the universities or companies whereas the remainder has participated in some online competitions. Some of the on-site competitions organized by the universities are Battle of Hackers (Asia Pacific University), Augmented Reality Security Forensic (Asia Pacific University), UiTM KiCTM CTF (UiTM), Dawg CTF (UMBC University – International) and internal CTF competition by the universities. Local and foreign companies that have organized the on-site competition are F-Secure, KPMG, MDEC, EC-Council, DEF CON Communications, Wizlnynx Group, SECARMY, VirSecCon and Cyber Sea Games. On the other hand, some of the websites that provide

online hacking competitions are Hack The Box, Hackathon, Hacker one, Secarmy, Skr ctf and VirSecCon.

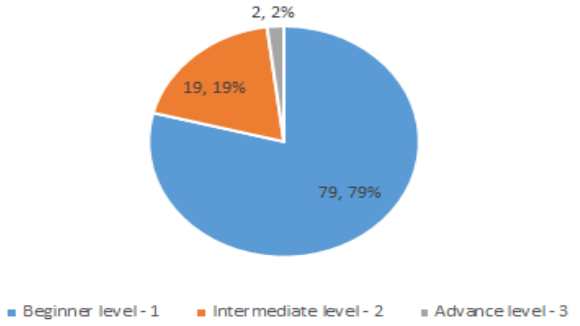

Fig. 9. Hacking Skills

The level of the hacking varies among the respondents as shown in Fig 9. 79% of them are at the beginner level, 19% are at the intermediate level and the remainder are at the advance level. This can be explained that 88% of the respondents are coming from the school and university level in which their level of exposure towards hacking and security as whole are still low as compared to those who have been working and exposed in the IT field.

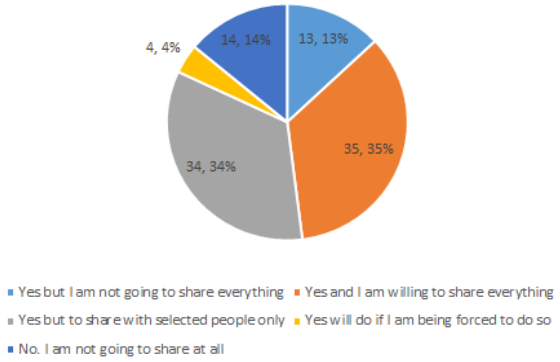

Fig. 10. Willingness to share knowledge

By analyzing the data collected on the willingness to share knowledge and experiences in ethical hacking (Fig 10.), results have indicated that 35% of the respondents are willing to share their knowledge with everybody. There is an insignificant of 1% difference between those who are willing to share their knowledge with selected people. 13% mentioned that they are not willing to share all the knowledge with others whereas on 4% are willing to do so if they are being forced. Only 14% indicated that they are not willing to share at all their knowledge in hacking.

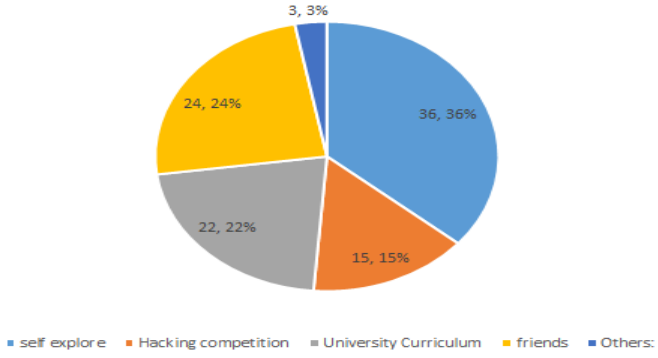

Fig. 11. Hacking knowledge gained

Based on the data gathered on the hacking knowledge gained as shown in Fig 11., 36% claimed that they learned the hacking techniques and skills by self-explore. 24% learned through friends, 22% learned through university's curriculum, 15% through hacking competition and 3% learned through other platforms such as seminars, workshops, attending courses and internship.

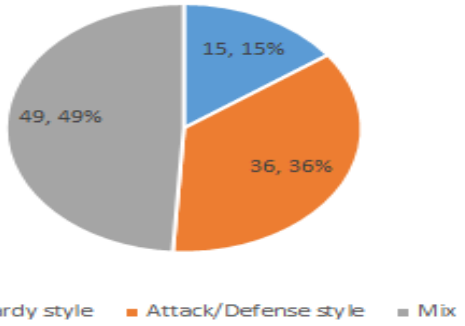

Fig. 12. CTF style preferred

By analyzing the data collected on the type of CTF style preferred as shown in Fig 12., 49% preferred mixture of Jeopardy and Attack/Defense style, 36% favored Attack/Defense style although this sort of style is ordinarily focused on those with more experience and are led at a particular physical area and 15% preferred Jeopardy style in which it provides a list of challenges and award points to individuals or teams that complete the challenges.

C. Psychological

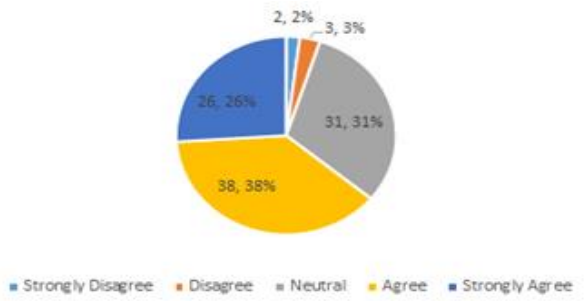

Fig. 13. Participants feeling towards hacking activities

Based on the responses gathered from 100 respondents as in Fig 13., 38% agreed that the ethical hacking experience left them feeling great. 52% from the respondents is neither agree or disagree when asked whether they felt that they are competent enough to meet the high demands from the hacking situation.

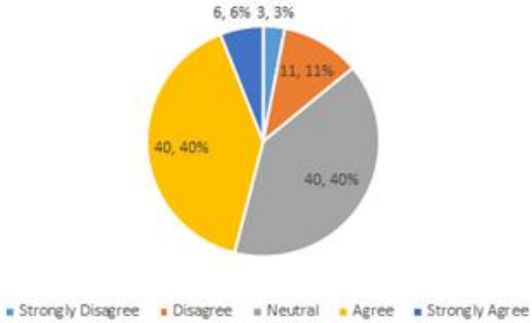

Fig. 14. Hacking is a challenge

When asked whether the respondents feel like hacking is a challenge but believed that the skills would allow them to meet the challenge, 40% of the respondents are neutral about it. However, it is interesting to found that another 40% of the respondents do agree to the statement (Fig 14.).

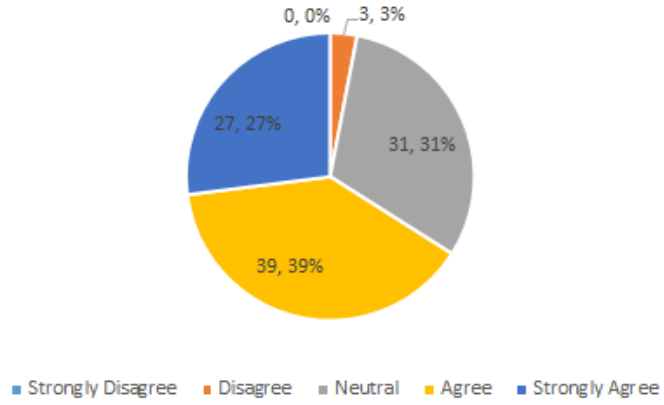

Fig. 15. Hacking experience is rewarding

Most of the respondents, around 39% agreed that the experience in doing hacking is extremely rewarding (Fig 15.). When asked whether the respondents attempt the activity due to some external situation which forces, 41% of them were neutral about it. Hence, the attempt to conduct the activity was neither due to forces or voluntarily. In addition to that, they were also asked whether they took the attempt because of their interest and enjoyment of doing it, the survey found 41% of the respondents condone to the statement.

We also asked respondents whether they attempted the exercise because they felt that it will help them to grow or develop in a way that is personally important to them, and the researchers found 40% of the respondents agreed to the statement.

Respondents were also asked whether they did the attempt because somebody else wants them to do it or they did it because they will get something from somebody, and the researchers found 39% responded neither agree or disagree to the statement.

IV. RESULT

Based on data gathered and analysis that has been done, the result that discuss in this section will be focusing in two area which are influence factors toward hacking and the millennial psychology impact.

A. Influence Factor Towards Hacking

Based on the survey that has been conducted, the researchers can summarised that there are four major factors that have influenced the targeted millennial to involve in hacking activities/attacks. The four major factors can be divided in two main categories that are external and internal factors. The external factors are as follows: academic background, numerous platforms to practice hacking and reward in participating in hacking activities whereas the main internal factor will be self-interest towards hacking activities.

Based on the statistics, 81% of the respondents are from public and private universities. Therefore, this group of people has been exposed to the hacking activities through the curriculum embedded in the course structure. The researchers have mentioned that to design the security programs for higher education level, the best is to emphasis on security training rather than security awareness. Students will be practicing more on hands-on learning rather that theoretical concepts. By exposing students to the correct methods and techniques in ethical hacking, have basically arouse their interest towards hacking activities. Furthermore, these universities, colleges and several organizations also have provided platforms for the students to test their knowledge and skills through competitions and seminars (C. Yoon et al., 2012).

According to the data gathered, the respondents have mentioned that there are numerous free platforms that are available for those who are interested with penetration testing or hacking activities such as Hack the Box (HTB), picoctf, Tryhackme and many others. These platforms have provided fun and yet challenging hacking exercises and online competitions for their registered users. By engaging to these platforms, users from various level of hacking background can participate and share ideas. These available platforms provide exercises or competitions for novice to expert level of hacking background. Users were also exposed to different type of CFT styles in order to enhance their hacking skills.

The third factors will be reward in participating in hacking activities. Having knowledge in hacking will encourage the respondents to participate in any hacking competitions. These competitions are not only organized locally in Malaysia but also several international competitions such as DEF CON Communications, Wizlnynx Group, SECARMY, VirSecCon and Cyber Sea Games. Most of the competitions will provide certificate, trophies or cash money for the several best teams' performance. The best reward of all is the experience gained throughout these activities. Therefore 66% of the respondents mentioned that the hacking experience are extremely rewarding.

The last factor that influenced the hacking activities will be self-interest. According to the statistics, 69% of the respondents stated that they attempted hacking activities because of their own interest and enjoyment of doing it. On the other hand, 74% mentioned that these hacking exercises have helped them to grow and develop in their own way. Therefore, we can conclude that, it is the self-interest that motivates many of our respondents to participate in hacking activities. Their self-motivation and enthusiasm will be the main factors that contribute towards their behaviour and interest towards hacking.

B. Psychological Impact

Based on the predictors used in the survey questionnaire to gauge psychological impact towards hacking attempt among millennial, the researchers can generalize through 100 respondents that the activity gives self-rewarding and challenge their knowledge and ability. It is increasing their level of self-esteem once they are successful in doing the attempt.

The relationship with monetary reward or were forced to do such activity is very minimal as their respond stated that they continue doing the attempt albeit any forcing factors, either internally or externally towards them.

Another strong psychological factors that contribute towards hacking attempt is interest and the "joy" of doing it. Most of the respondents condone to the statement. This demonstrated a strong inclination of doing the attempt to fulfill self-satisfaction and to prove their ability.

Overall, based on the responses gathered from 100 respondents, the researchers can summarize that generally, for young people, aged between 20-24 years old, the most significant psychological factors that entice them to attempt hacking activity is to prove their ability and full fill their self-esteem which will bring "joy" and satisfaction to their live.

V. CONCLUSION

Millennials are those who grew up using electronics devices and the Internet. They spend more time on their smartphone, accessing internet for online gaming, social media, online shopping, viewing YouTube any many others online activities.

The most common attacks based on current trends worldwide are social engineering, malware attacks and web-based attacks. These types of attacks being studied in detail to relate the millennial activities towards hacking activities, penetration testing and hacking competition.

A survey conducted to targeted millennial group in Klang Valley area with 100 respondents responded to the survey. The questionnaires being designed to gain information on demographic, hacking experiences and psychological of the millennial towards hacking activities. Based on data collected analysis being done to come out with the result. The result is to identify the millennial influence factor and their psychology impact towards hacking activities.

Based on research and analysis that being conducted, the researchers have found that there are two major influence factors which are internal and external factors. Internal factor is the millennial interest towards hacking activities while the external factors are academic background, numerous available platforms to practice hacking and reward in participating in hacking competition or activities.

Psychology impact towards hacking attempt among millennial shows that the activities give self-rewarding and challenge their knowledge and ability where this will increase their self-esteem. Most of the millennial participating in hacking activities or competition due to their interest to fulfill self-satisfaction and to prove their ability intentionally or unintentionally.

REFERENCES

Brewster, T. (2020). *It'S Worryingly Easy To Spam Fake Government Coronavirus Warnings Direct To Populations' Phones*. https://www.forbes.com/sites/thomasbrewster/2020/03/27/its-worryingly-easy-to-create-fake-government-covid-19-warnings/#198792784e50

C. Yoon, J. W., H., & R., K. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, *23*(4), 407–416.

Help Net Security. (2020). *COVID-19 has contributed to record breaking cybercriminal activity*. https://www.helpnetsecurity.com/2020/05/14/covid-19-cybercriminal-activity/

Karaffa, C. (2017). *Causation and Impact of Ransomware Infection in Large Organizations*.

Kaspersky. (2020). *Top 10 Most Notorious Hackers of All Time* . https://me-en.kaspersky.com/resource-center/threats/top-ten-greatest-hackers

KnowBe4. (2019). *Security Threats & Trends Report* . https://www.s3-uk.com/knowbe4-security-threats-trends-report-oct-2019/

Lomte, R. M., & Bhura, A. (2013). *Survey of different Web Application Attacks & Its Preventive Measures* (Issue 5). www.iosrjournals.org

Nao.org.uk. (2020). *Wannacry Cyber Attack And The NHS*. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

Netscout.com. (2020). *NETSCOUT Threat Intelligence Report*. https://www.netscout.com/sites/default/files/2019-02/SECR_001_EN-1901%20-%20NETSCOUT%20Threat%20Intelligence%20Report%202H%202018.pdf

Owasp.org. (2020). *OWASP Top Ten Web Application Security Risks | OWASP*. https://owasp.org/www-project-top-ten/

Packt. (2019). *Understanding the cost of a cybersecurity attack: The losses organizations face*. Understanding the cost of a cybersecurity attack: The losses organizations face

Purplesec. (2020). *The Ultimate List Of Cyber Security Statistics For 2019* . https://purplesec.us/resources/cyber-security-statistics/

Sobers, R. (2020). *Must-Know Cybersecurity Statistics For 2020* . https://www.varonis.com/blog/cybersecurity-statistics/

Tasril, V., Br Ginting, M., Mardiana, & Siahaan, A. P. U. (2017). *Threats of Computer System and its Prevention*. www.ijsrst.com