Cheng Hu

Intranet Security
Overlooked Importance

Bachelor's Thesis
Information Technology

December 2013

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Date of the bachelor's thesis** 29 Nov 2013
Author(s) Cheng Hu	**Degree programme and option** Information Technology

Name of the bachelor's thesis

Intranet Security

Abstract

The aim of the study is to find out how does vulnerabilities affect intranet security and credentials in a small enterprise environment. Due to low Local Area Network security level will probably leave exploits and loopholes that could be utilized by attackers and eventually lead to data loss or credential leakage. Thus the research was carried out by studying on principles from typical attack representatives that were divided into both 'offline' and 'online' groups. Research was followed by one case study on an attack which originated internally from an enterprise, gave strong support to the importance of intranet security viewpoint that holding by previous theoretical studies.

One whole process of attacks over LAN was designed and implemented within laboratory environment to verify the study. The series attack contains network join, exploits discovery, and penetration implement phases. The laboratory work was finally achieved by logging target victim's personal credentials.

Within Network join phase, wireless attack on WPA/WPA2 secured Wi-Fi signal with WPS function on was taken and layer-2 attack turns intruder into man-in-the-middle and got the relatively higher privilege than a regular network user. Genlist, Nmap, and Nessus was used to make full network scan in order to detect the intranet topology. Phishing was the main character in the penetration implement phase, thus milder attack method like web cloning, DNS fraud was utilized rather than offensive ones. In the end, the key logger in the back end captured the credentials from target victim successfully and the possibilities of migrating the attacks to mobile devices was analysed.

Subject headings, (keywords)

Intranet, Network Security, Virus, Malware, Worm, DoS, DDoS, Penetration, WPS, MAC Flood, ARP Spoof, DNS Fraud, Web Clone, Phishing, Social Engineering

Pages	**Language**	**URN**
36 pages	English	http://www.urn.fi/URN:NBN:fi:amk-2013120520154

Remarks, notes on appendices

Tutor	**Employer of the bachelor's thesis**
Matti Koivisto	Mikkeli University of Applied Sciences

CONTENTS

1 INTRODUCTION 1

2 GENERAL NETWORK ATTACK METHODS 2

2.1 Trojan 2

2.2 Worm 5

2.3 Denial-of-Service (DoS) 8

2.3.1 Attacks Static Properties 9

2.3.2 Attacks Dynamic Properties 11

2.3.3 Attack Interaction Properties 13

2.4 Phishing 14

3 LESSON FROM REAL CASE 18

4 LAN ATTACK PROCESS 21

4.1 Network Join 21

4.2 Exploit Discovery 22

4.3 Victim Maintenance 25

5 SERIES ATTACK SIMULATION 26

5.1 Creep into the environment 26

5.2 Familiarize with the environment 29

5.3 Spoof & Fabricate the environment 31

6 CONCLUSION 35

BIBLIOGRAPHY 37

1 INTRODUCTION

Within the trends of rapid development in technologies, network security became a hot topic that being widely discussed globally. To avoid massive attacks over Internet, by choosing to install firewalls and anti-virus software, enterprises or individuals believe their intranet would be secured safely. Unfortunately, relative than using traditional ways like compile Trojan or worms and spam them out, attacking methods are tending to become more insidious and hard to be detected from internal networks (ex. Phishing, Social Engineering). This brought the security threats closer to a network's backyard (Local Area Network) rather than the semblance (Wide Area Network).

The aim of the study is to find out how does vulnerabilities affect intranet security and credentials in a small enterprise environment. This would help to prove the equivalence of the information security importance on either against external invasions or internal penetrations.

Several representatives of the typical network attacks, which including both offline and online methods would be analyzed. This would help to understand modern network attacks evolution and further possible trends, as is the theoretical aim of the study. All these studies would be covered in the next chapter.

Real life case that happened on intranet security negligence would be extremely strong support for the sense of this thesis study. Thus, one heavy case study would be carried out in chapter three along with objective analysis.

From previous two theoretical studies chapters, common network penetration process needs to be concluded in chapter four, as to guide and help to give ideas on designing the practical study process in the following chapter.

In chapter five, a series attack that starting from sneaking into a network all the way till the end as utilizing the security flaws would be fully implemented in the laboratory and explained specifically. In the end, there will come up with one conclusion chapter to cover the ideas that had been studied, and what had been learnt and summarized.

2 GENERAL NETWORK ATTACK METHODS

Innumerable network attacks appeared since the concept of networking had been introduced. However, diverse methods all tend to obtain the same results substantially. In general, their goal is to gain to the relatively high privilege through an illegal way, in order to have rights to deploy the data which should not be touched, apart from administrators.

To understand several typical representatives of the potential security threats would possibly help for preventions. Additionally, there are two ways of attacks, which are either offline or online. Hence, the study selected two most common instances that are almost experienced by any individuals and enterprises for each attack method respectively, which are Trojan and worm for offline, besides DoS and Phishing for online.

2.1 Trojan

Trojan, one of the most famous malware ever. It does not duplicate itself commonly like other viruses. With gaining unauthorized relatively high privilege to creep into the victim's host operating system (OS), it usually generates and bundles with single or several malicious payloads; in most cases, backdoors will be included in order to give accessing privilege to illegal remote connections after the first time. Most backdoors will slow down the host OS operating speed considerably. However, unlike general computer viruses, most Trojans would not favor the adsorption to other files and do injections. Instead, they would rather be considered the janitor typically in nowadays series attacking process. Illegal high privilege will give Trojan utilizer most possibilities to sniff, steal or even destroy the host OS. Thus, it could be quite sneaky and hard to be detected without a sample database on anti-virus software.

Trojan is a term that derived from Greek mythology, Trojan horse in Homeric Hymns (FIGURE 1). Similar to the menace hiding inside a wooden horse, malicious codes are well compiled and posed as useful programs that are completely harmless in order to convince victims download and execute them. One of the earliest Trojan was exposed in 1986, it was posed as the 2.72 version of one sharing software, PC-Write. When users trusted the software they have, and execute it, their storage will be formatted by the

malicious code that came along within the Trojan. The irony is that, Quicksoft, the author of PC-Write, had never released version 2.72. [2] In a sense, this is the first generation of Trojan, which had no infectiousness strictly.

FIGURE 1. Trojan horse in Homeric Hymns [1]

Not so long later, in 1989, Trojan AIDS was exposed. Emails were not as popular as nowadays back then. The author of AIDS was sending traditional mails out that attaching the Trojan on a floppy disk. Reason for calling the Trojan AIDS was because the mails were describing medicine prices, precaution that related to AIDS and HIV. When the Trojan was executed from floppy disk, instead of getting storage formatted as what PC-Write did to users, the storage will be locked up and noticing victims to pay for a unlock. This is a typical representative of the second generation of Trojan due to its contagious property in comparing with the first one.

Starting from 90s, Internet became more and more commercialized to public. [3] Huge number of users led to its rapid booming. Convenience had been brought to users for their daily life as legal use, however, it benefited viruses simultaneously. New generation of Trojans combined features of both camouflage and dissemination, easily spreading out through TCP/IP. It also introduced new features which was not included previously. Started from then, Trojan has the concept of backdoor so it could be utilized by crackers to re-connect to victims. Either, key-logger was introduced so personal privacy started to leak out, especially there was only few accounts back then for personal use. Emails could be used as spamming tool illegally.

Even though nowadays Trojans are existing almost everywhere on the Internet and they all complied differently, but their concepts are still as similar as the third generation which had been mentioned. As their principle of functioning is to be initiative to connect to external interfaces, thus they are relatively easier to be detected once they starts working even though they are well compiled to escape the first round of scan by anti-virus software. At least most of the anti-virus software will notice the system user, there has been one suspect process trying to connect itself out to random rare ports.

In connecting to the host OS remotely, crackers can most likely have full control to the victims (ex. window capturing, transfer files, modify OS settings, steal personal finical account information, etc.). Being hijacked by such virus would be concluded as hijacked by malware. Trojan existed as one of the most famous representatives had never been completely eliminated, but tragically became a perfect prototype for people whom have sinister ideology to carry out their deeds.

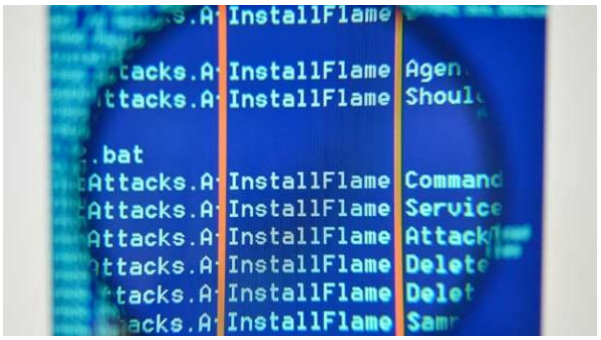

FIGURE 2. Flame [4]

Flame, as one of the newest malware which targeted most likely Middle Eastern countries as cyber spying purpose, had been exposed to public in 2012 (FIGURE 2). [5] Infected OS would try to be contagious via Local Area Network (LAN) or Universal Serial Bus (USB). By utilizing the privilege it gained illegally, any protocol of transmission will be tried to activate to download contacts information, Bluetooth was reported as one of the way to get nearby information. After the information were collected and packed up in hidden, these packets will be uploaded to remote servers all around the world to get prepared for the next usage. Considerably, more than three-fifths infectors was discovered in Iran, Israel, Sudan, Syria, Lebanon, Saudi Arabia, and Egypt. [6] This malware had also been reported in North America and Europe. [6] The malware had influenced innumerable victims including governments, businesses, individuals, even educational institutions. Some people hold the point of view which criticize the

U.S. government, as the biggest suspect, should pay responsibility to the Flame. As one for ‘supervising’ on ‘potential threats’ originally but ended up with brought personal private information leaked globally, especially in Middle Eastern countries, speech about religious conflict was also being trumpeted by conspirators. In fact, Flame had stopped functioning or being reported dramatically less after its exposure to the public. This was suspected as sending ‘suicide’ code to itself (as known as ‘kill’ command) but indeed by the ones behind the scene. Also, the efficiency and helpfulness on anti-virus software, as well as the rigging with governors especially after Edward Snowden event, has become a hot topic not only once.

2.2 Worm

Worm, as one of the most famous computer virus. It has a very strong ability of self-duplication. Very different from Trojan, one of its main feature is spread the files that containing malicious complied codes out to other directories on host OS or even to other OS through network automatically. As same as other viruses, worm has all the common payloads (ex. Deleting files, encrypt unauthorized files, spam data through email, back-door, etc.). One of the very first reason to define it as ‘worm’ was because the virus will show as a graphical worm to ‘eat’ or change letters under DOS system on outbreak back then. Yet different than other viruses, worm does not need a host program or process on OS, it will try to copy and infect itself out to others (either locally or through network). As soon as it found and infected the ‘next’ victim, it will commonly terminate itself so the suspicious process is vanished or changed. Most common used port for worms is 1434. Worms usually consumes quite a lot network resources so there is only few left for other processes that need network resources too.

As one of the famous Chinese worm raged in 2007, Worm.whboy (FIGURE 3), which was utilizing the exploits on Microsoft Windows, all infectors were continuously dialing on DSL (most common way for internet connection in China back then) to consume large computing and networking resources. As well, it will look for any network address in infected files and file sharing function for next step propagation. Eventually destroying most of the victims’ data. [8] This was also the first biggest case on virus that Chinese police had investigated (since writing or spreading virus code deemed as crime in Chinese law). Ironically, the worm’s representative ‘whboy’ (where ‘wh’ indicates

"Wuhan", a city name, as well as the worm author's location) became the breach for police.

In fact, worms, from the very beginning, was not released with malicious payloads like backdoor or destructive codes as the real intension. Instead, it was released as a 'tool' to measure the scale of the Internet with its duplication feature, expressed by the author Robert Tappan Morris back then (the first worm was also named after Morris). [9] However the Morris Worm was released from MIT instead of Cornell University even though the author was from the latter. Morris Worm made the infected files keep on infecting other files within the OS due to the syntax error that had been made during the origin programming. This made the Worm more harmful indeed. Every time it infects others (sometimes itself), self-replication would consume a lot resources, which directly reflected as slowing down the victim OS's operation (this might be a Web or network server, or individual computers), as same as how slow the worm squirms. Morris Worm cost around $200-53,000 to get removed on each installation by U.S. Court of Appeals [10] and himself became the first person get convicted. [11]

FIGURE 3. Files had affected by Worm.Whboy (Panda figure) [7]

Almost one-fourth century after Morris convicted in 1986, [11] again, in Middle Eastern country, Iran, received one infamous worm: Stuxnet.

Many famous anti-virus enterprise including Symantec, Kaspersky Lab and many other ones discovered a computer worm which mainly focusing on infecting industrial controlling system in mid-2010. Stuxnet, as which had been widely believed to be the results of cooperation between U.S. National Security Agency (NSA) and Israel. [12] This was also believed as targeting on Iran's nuclear facilities since the simple investigation report from Symantec declared around 60% of the infection was detected in Iran, 20%

in Indonesia and 10% from India. In addition, Azerbaijan, Pakistan, and the U.S. were also shown with few cases. [13] Stuxnet was also believed infected Chinese networks that led six million individuals and over thousands cooperate accounts across the country suffering. [14]

Stuxnet was not functioning as a regular virus that target on stealing personal information related to any finical purposes. That is why someone pointed out it was not as usual as a common virus and further study on it verified it is more complicated than a normal virus that individual hackers or even a simple team could accomplish. It utilized five exploits in total from Microsoft Windows system plus two from Siemens SIMATIC WinCC system before they were fully patched. [15] In fact, four exploits on Windows system were Zero-day exploits which are extremely valuable for special purposes. Due to this, hackers will not being stupid enough to waste any single one of them to do tests, let alone all four on one Worm creation. Additionally, with infected USB drives initially, Stuxnet will attack WinCC system that exists in the victim's network. [15] Because of password changes will negatively affect industrial process which Siemens suggested to users, some of them was bungled due to this 'advice'. In another word, the author of Stuxnet has to be extremely familiar with either industrial fundamental facilities or manufacturing process. [16] As well, they have to master a lot knowledge about data transmission principles and information technologies. Additionally, programming language is essential to produce such complex and large virus files (including at least C and C++). Significantly, the virus was target on special industrial field which means it is does not apply to anyone but only to those special distinctive industry, most believes nuclear facilities, which is nearly impossible for ordinary individuals to touch with. To sum up, rather than utilizing the exploits to create simple Worms to troll money, Stuxnet needed huge investment and human resources paying by innumerable studying and working hours. Eric Byres, whom is well experienced in trouble shooting and maintenance work on Siemens industrial system expressed to magazine 'Wired', to write and compile all these codes might consume a huge experienced team by several months, even years. [17]

"Stuxnet is a working and fearsome prototype of a cyber-weapon that will lead to the creation of a new arms race in the world," Kaspersky Labs said the attack could only be conducted "with nation-state support". [18][19][20] Russian representative at NATO was expressed on 26th January 2011, the Stuxnet virus might cause serious influence to

Bushehr Nuclear Power Plant at Iran, it might led to the leakage of toxic radioactive material, the negative effects will not be less slight than the Chernobyl disaster that happened in 1986. [21]

Either Trojan or Worm virus would cause serious security problem. Either for individuals or for nations or even for human race, confusion in the virtual world would sometimes step into the physical real life. It could also be as worse as a war disaster.

2.3 Denial-of-Service (DoS)

Trojan or Worm are very typical representatives of malware or virus that distributing through the Internet, but could only get user infected if they execute them. Anti-virus software and firewall installation cannot heal these two fundamentally, while, at least they would help to slow down the infection process. This situation has created a lot of people misunderstanding that it is secure to lay back behind the anti-virus software and firewalls if they do not execute anything. In reality, those one-sided and careless ideas had never brought them any benefits or conveniences. ‘Trouble’ sometimes ring your doorbell or even break in themselves through network.

To interrupt or suspend the process that intended users or clients connecting to a web or other networking services, denial-of-service (DoS) attack is an infamous solution. Target on consuming most networking resources of the victim is actually one of many DoS attack ways. As soon as the attack could send victim into trouble or pause it from providing services even get dumped, it might belongs to DoS attack category. In some certain cases, attack is hard to work with single or limited computing resource (ex. To attack finical agencies, huge enterprise network, medium scale of web servers). Just like single stick would easier to break than a bundle of them, hackers would prefer to join quite much computing resources together before starts the attack (as known as botnet).

When a group of victims from previous hacks been putting together and commanded to do the same job towards single target, the services request it generates might be unthinkable massive. Hence the target will be overwhelmed and run out of resource to keep on providing the service. This can be imagined as a massive group of panic-stricken people trying to squeeze into the regular door at the same time (this is why the botnet is defined as zombie network as well). Every single node from this botnet is one

victim under hackers' control. They might geo-located differently but all 'contributes' to the attack. As same as cloud service having distributed servers in the network, this attack is considered as Distributed Denial-of-Service (DDoS) attack (FIGURE 4).

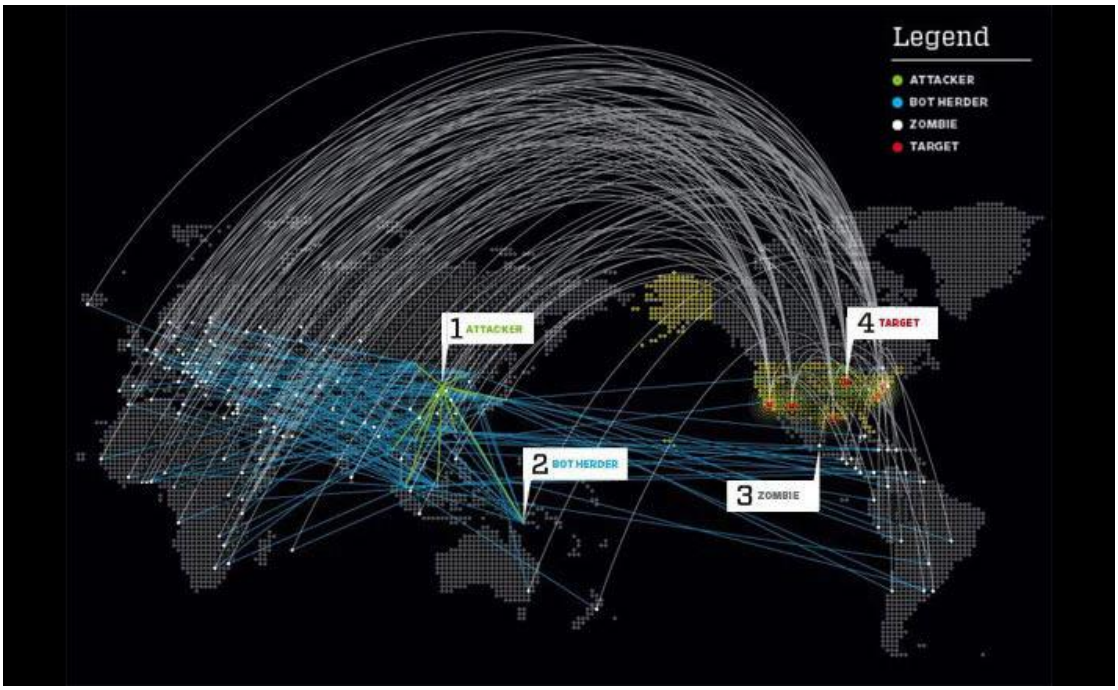

FIGURE 4. DDoS Attack Principle & Visual Effect [22]

Thus, the ways of initiate a DoS attack might various in order to achieve diverse goals. Generally speaking, DoS attacks can be identified with three key property categories mainly, which are static, dynamic, and interaction. [23] By analyzing the properties which DoS attack have, they could be classified specifically. The properties that usually will not change during one continuous attack, which generally had been settle down before the attack, is called attacks static properties. This is determined by hackers and attack itself, which is the fundamental properties. On the other side, the properties that could change during the attack is known as attacks dynamic properties (ex. Target, Timing, Node selection, etc.). In the middle, properties that not only related to the attack initiator but also restricted by the specification, security scan, and ability for providing services from the victim's side, is defined as attacks interaction properties.

2.3.1 Attacks Static Properties

Static properties are usually contain Attack-Control-Mode, Attack-Communication-Mode, Attack-Technical-Principles, Attack-Protocols and Attack-Layers.

Attack-Control-Mode

The controlling mode will restrict the secrecy of attack source strictly. Suiting different attacking methods, victim control mode can be classified as mainly direct, indirect, or auto.

At the early stage of DoS, from target settle down, attack implementation to the final termination, attacks were usually set up manually by the hacker. This is relatively easier for externals to track and do investigations. This brought danger to hackers thus the attacks were started to use multilayer structure. Strait hierarchy method brought great amount of work to trace back to the original hacker, which is still been using nowadays, as well as the auto mode. The attacking methods was already been set up before virus was compiled and released. The drawback of this mode is, it requires a lot technical backgrounds from attack initiator obviously.

Attack-Communication-Mode

From the indirect Attack-Control-Mode, there could be many ways of communications between attacker and victims. These ways would judge the difficulty on tracing back. Generally can be understood as bi-communication, mono-communication, or indirection.

Former means the data packets that victims receive contain the upper attack hierarchy's real IP address, which can be easily trace back. Second way means the hacker's real identity information will not be included in the data packets that sending to victims, usually fake IP address will be added into UDP packets before sending. This way brought plain difficulty to investigators to trace back, only with marking the acknowledgement packets would help. However, there are several limitations for using this communication way, such as the hacker is hard to supervising the victim on its feedback and status. The latter, indirections, as one special way of bi-communication, utilize the third party to comply sessions with victims. This way is concealed, hard to trace back or supervising and filter. The records that victims logged is very limited (sometimes only back to a random public server that for intermediate communications). This way is quite common through Internet Relay Chat (IRC) since August, 2008. [24] Hacker groups will connects to a random IRC server to send the commands towards victims.

Attack-Technical-Principles

Semantic and Brute are basically two main principles that have been using actively. Semantic usually utilize the existing flaws and loopholes to do DoS attacks. In reality, it does not requires hacker for much networking bandwidth. Under certain circumstance, even one packet would collapse the target. Meanwhile, victims could easily avoid this type of attack by doing regular patches or updates.

Brute method does not requires the victim has exploits itself, but by sending huge quantity of service request to the victim to run out its resource and destroy it (as known as storm attack). To avoid this type, with the own power from victim side is not enough. It also requires the router from upper layer of the victim (can be ISP) to have filter functions. Certain attacks combine these two principles together to make themselves even stronger against solutions (ex. SYN Flood.). Even, some attackers are familiar with the physical or protocol flaws existing in the victim's designs so the attack would even generates more dataflow to crash the victim. This seems one of the brute attacks but can be fixed only by fixing the flaw in design or protocol first, thus, someone believes that is a typical semantic attack as well.

Attack-Protocols

Massive protocols will be involved during one continuous attack, such as SMTP, ICMP, UDP, and HTTP from the top layer. In principle, the higher layer from where those protocols that involves, the more resources it will consume of the victim to do analysis on the packets that attackers sent.

Attack-Layers

Usually attacks with TCP/IP are from layer datalink, network, transport, and application. Attacks on datalink layer (as known as Layer-2) will only happens within LAN due to the restriction of protocols. It is rare to see but easily get overlooked. Most attacks are targeting on network layer, as well as application.

2.3.2 Attacks Dynamic Properties

Source-Address-Type, Packets-Data-Generation, and Target-Type are mainly three property categories for consideration.

Source-Address-Type

Attacks initiator would chose to use true, forge legal, or forge illegal types as their source address. As mentioned above, true IP address can be used but easier to get trace back. Forge ones would solve this challenge, either increase the difficulties to victims for doing packets analysis and filter. However, in some cases, true IP source address need to be used. Due to its high possibility to get the source information exposed, the rate of using it is sliding down in recent years. Forge address are typically the ones that had been already assigned to legal users but going to be re-used by attacker illegally for the second time; or the ones that reserved in the network which had never been assigned to anyone.

Packets-Data-Generation

Data inside the attacking packets are mainly existing in five different modes, which are none, unique, random, dictionary, and function.

As the process during storm attack mentioned previously, attacker need to send massive packets to the target. The data information load inside the packets can be generated with different modes. Different modes will affect the victims on their checks and filter actions to the packets. Packets load could be generated by four different ways. First, sending the packets with same loads. This kind of packets will have typical characteristics which can be detected on the first hand. Second, send the packets with random loads. Even though these packets can be possibly recognized by 'Mode recognition', easily get filtered out due to most of them are randomly generated without practical meaning, but the attacker can still design the way of the random generation. In this case, victim would recognize the packets contain malicious information till they analyze to the application layer, which made it harder to get filtered considerably. Third, attacker will picks up certain ones they think is meaningful every time it forms up by following certain rules, in order to add up a packet set. This is hardly working for victim's checks when the scale is small. Fourth, the last way is to generate different load every time. This is quite hard to conclude since each function that using for generation various, will eventually led to different difficulties in detection.

Target-Type

Attacker would choose the target randomly, but most likely they are application, system, critical networking resource, network, network infrastructure, or Internet.

The most common way to do attack is focusing on the applications. They usually target on one certain application's loophole and keep on doing DoS attacks. To run out the victim's resource is quite typical case for systems (like SYN storming, UDP storming). Some attacks are just target on critical resources, this might including Domain Name Server (DNS) or routers especially. While the ones that targeting on the network must holding enough resource and techniques (generally root domain server, trunk core router, famous digital certificate server). This type of attacks are not very common in practice but definitely a fatal one if it happens. Target on Internet means a worm or Trojan that will massively spread all over, which lead to huge number of hosts, networks having Denial-of-Service effect. This type would brought almost the worst damage.

2.3.3 Attack Interaction Properties

Either the static or dynamic properties of attacks are not only restricted by its initiator's implementation methods and abilities, but also limited by the target users' ability. This might mainly contains detectable possibilities and attack effects.

Detectable-Possibility

Victims can be categorized by their abilities for detecting malicious packets, filterable, unfilterable, and Noncharacterizable.

Sometimes, to victims, attack packets have quite typical characteristics to be detected. Attack defense could be implemented efficiently to keep service providing normally by filtering these packets. However, the characteristics that had been added in the filter could affect regular packets simultaneously as well, even affect normal service providing. This is exactly the same goal as what attacker want to achieve. Thus, in a sense, by adding those characteristics to the filter blindly will not work out. The worst situation is the attack packets has no such typical particularity than normal packets. This would lead the victims to fully exposure in front of the hackers attack packets.

Attack-Effect

Different levels of attack effects, from none, degrade, self-recoverable, manually-recoverable, to non-recoverable, will help to classify all victims.

If the target system can still providing the same service as it was during an attack, this could be defined as no effects. If the attack strength is not enough to creates fully DoS

but by slowing down a bit on servicing ability, degrade is a fair title for these attacks. When the attack reaches the scale to generate a full DoS, it means the service damage is successfully made to the target. Typical DDoS attacks like storm categories will not cause serious effect to the victim. They are usually self-recoverable. To utilize some of the loopholes on the system could crash, restart, or suspend the server. Starting from there, target victim might need to call engineers to do manual-recovers. While some other attacks are directly destroying system files on the target, it might led to the critical data loss. In this case, the server might not providing same services even after they are manually rebooted.

In fact, not only rage on Internet, DoS attacks sometimes prefers LAN better since they have exploits being overlooked but can be utilized sharply. Layer 2 appliance (from OSI model) configurations would betray the whole security system been set up. ARP spoofing, MAC flood are all typical representatives.

2.4 Phishing

Starting from Trojan, Worm, to DoS attacks or DDoS attacks, active attack methods have been using for over couple of decades. Any servers or individuals that exposing under Internet are quite vigilant. Qualifications that set for packets scanning and filtering are extremely tight and intelligent as possible. This practical situation limited the active attacks not deadly but almost. It is in this environment, people starts to dig more possibilities from side to side. Then some of other attacks that love to hide in shades with great invisibilities stepped into hacker's sight. Phishing attack techniques, as one of them, was first introduced and archived in 1987. [25]

Phishing is a technique that trying to hide the hacker's real identity to steal personal sensitive information (can be bank account, credit card information), by disguising itself as a famous third part which has great credits. They all commonly declare themselves as one of the biggest e-commerce (ex. eBay, PayPal, Amazon, etc.) to gain the trust from users, so the users would unguarded themselves and speak their private information out eventually. Most common way for spreading phishing information is emails, sometimes through Instant Messaging (IM) as well. [26] Almost the exact same login interfaces were cloned by hackers and be present in front of end victims, so they will not tell the difference and firmly type their private information in there. Even though

cryptography protocol Secure Sockets Layer (SSL) are used for identifying the server that currently providing the login service, it is still very hard to detect, recognize, and totally avoid phishing attacks.

In early years, hackers were doing phishing to get personal information on AOL due to the purpose of exchanging pirated software. [27] Before 1995, users could do registration on AOL with fake credit card numbers that generated by certain algorithm; however this 'loophole' was patched officially afterwards. [27] To keep on being active on AOL and get illegal copies on software, hackers set the trap web and started to spamming emails out to real AOL users so that if someone believed in the story they made in the email and leak their personal information out (usually type the username and password because of the 'verification request' in the spam), they will use that for further movements. Fortunately, AOL add a line "no one working at AOL will ask for your password or billing information" on their IM to stop their loyal users keep on getting deceived. In fact, credit card information within AOL account that being defrauded could be used by hackers in other fields for other purposes. E-gold, as a failure for doing attack against online payment system in June 2001, was also a first time attempt on putting 'further movements' into practice. [28]

By spamming emails out can only receive quite limited results. The sense made by felling and sharpening the axe, made hackers spent more time on gathering and optimizing target information before sending the emails out (as known as Spear Phishing). As another way for making the phishing email looks more realistic is, based on the previous real email sent by an official source, tiny modifications will be made to it. This might contains changing the hyperlink hide under plain texts. In practice, victims sometimes will not be cautious if they see the email is exactly the same as what they had received before from the official sender. Sender's email address are usually showing as a name or a group instead of true email address format, besides users may not verify if the hyperlink will lead them to where they 'thought'. This type of phishing is still being widely use nowadays (as known as Clone Phishing). When all these kind of phishing attacks are targeting on end talents in all aspects in the society, hackers would love to define it as Whaling. [29]

Nowadays, phishing techniques become more and more sundry. Hackers are definitely taking it serious because they believe in victims are smarter and more careful at what

they click on. Thus, a ‘word game’ like word by word, phrase by phrase are playing by hackers to conjecture what will victims reacts when they seeing the link. A good link manipulation will considerably increase the chance that others ‘take it’. Under the network environment that filled with anti-phishing browser plugins, hackers will shift from text to images so phishing filters cannot detect it correctly. Additionally, programs that can inspect a website comprehensively, are becoming more and more intelligent. They will learn from the target website carefully and download all they could from it (ex. Images, soundtracks, forms, text paragraphs, etc.). By putting everything back together, a cloned target website will be ready to cheat on victims. What victims seeing is not really the true website they wanted to go to, instead, it is a ‘pirated’ version. As soon as they starts signing in, log server will catch the sensitive information and forward it to the email address that had been set up already beforehand by hackers. Web clone (as known as website forgery) [30] usually targeting on the ones with login interfaces. Hence, social media web group is always the first priority hackers would take a consideration (FIGURE 5); as email servers will be the second one.

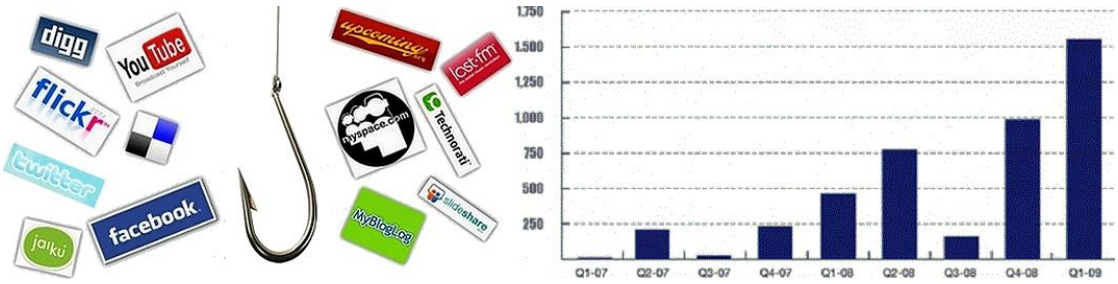

FIGURE 5. Phishing Attacks against Social Network [31]

When people already get used to the online tricks and become cautious, the one combines offline techniques would push victims one step forward. Spam containing hypocritical safety tips will deliver to victims’ inbox. Instead of asking them click on an awkward link, a phone number will be provided. [30] If user believed in a phone call account verification, hackers would probably seize the sensitive information successfully again. Phone number that provided is generally a Voice over IP (VoIP) number. Series questions would be asked targeting on sensitive information. In addition, hackers would like to legitimate the verification process by utilizing voice phishing technique. [32] Phishing techniques are innumerous and evolving rapidly. No matter which way hackers are using, the goal they have is always the same, personal sensitive information. According to statistics, considerable phishing servers are powered by earlier Apache

version (FIGURE 6), and two-thirds of them are hosted on UNIX platform (FIGURE 7).

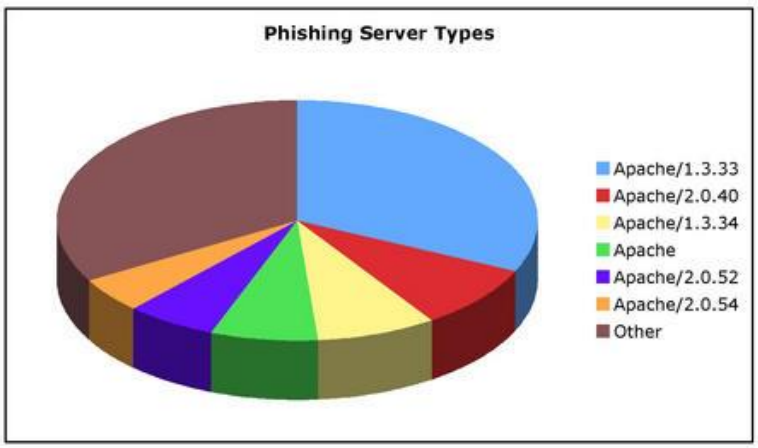

FIGURE 6. Phishing Server Environment [33]

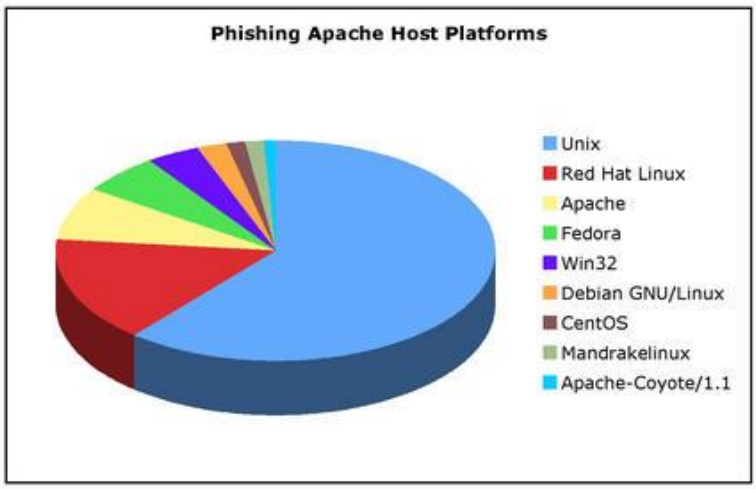

FIGURE 7. Phishing Apache Platforms [33]

Not by attacking on unpatched loophole, not by utilizing original design flaw, phishing is quite different from active attack methods. Instead, it does not requires too much technical background to initiate a possible attack which probably will bring great loss to the victim. Indeed, it is one of social engineering method that utilized users' diverse mentality. Instinct, curiosity, trust, greed, and many others all might brought danger of psychological traps to end users. Internet users are more or less tend to believe in giants in IT industry, Google, Microsoft, Apple, Facebook, Twitter, YouTube, they all holding great amount of users' private information in their hands. Certain amount of people would not use different usernames and passwords for each website, this gave hackers huge possibilities to get the information they want. Single webpage verification spam

might not work, but hard to tell on disguise as administrative letters from every single one. Sometimes, when one target is over hard to be hacked, victim's friends or relatives might became the pre-target since social networks are highly developed and there always will be a breach. Unfortunately, right imbalance and credibility crisis might be the biggest threat. When users believe in what the IT service giants provides, and link all their personal information and wealth up with it, possibility of totally prevent attacks from social engineering methods became less and less. Individual hackers or groups can probably make damages, but the number is still limited. Once a system started to abuse their power to bribe or threatening at IT giants, innumerable personal privacies and wealth would turn into nihility in front of its excuses which almost equivalent to jokes. Huge interests gathered together by trust, will eventually sacrificed in front of specific system's interests necessarily. When the so-called defender of the network order turned into a burglar acts recklessly, the definition of network attacks or social engineering will stays that pale. To large group of users that exposing under such a network environment which lacking of credibility, either the development of the network brought convenience and danger simultaneously or not, is a subject that far more complicated than it supposed to be.

3 LESSON FROM REAL CASE

Various typical network attack methods were analyzed specifically in the previous chapter. To administrators, the first priority is obviously study on preventions. This is quite similar to a simple cycle between mice and cats. Sadly, the story is always ends up with the success of destroy and massive remedy. This is like warns would hardly be learnt before mistakes are made. Flaw in the plan, quite many preventions are made to against external invasion, any internal omissions will probably be utilized by attackers to generate number of loss.

Starting from 1st July 2005, China Mobile Beijing branch office keeps on receiving complaints from users about the prepaid vouchers they brought usually expires before promised. The office sent staff to voucher database center to report and investigate the case. What made them stare dumbfounded, shortly within four months, 6,600 prepaid vouchers pin code had been modified illegally, they worth more than 3.7 million Chinese Yuan. Case was handed to Beijing Police Department immediately and marked as the first biggest theft on telecommunication charges in China. [34] After more than one

month investigation, police locked the aim on an engineer, Cheng Zhihan, at Shenzhen. By the end of August 2005, suspect was arrested and admitted on his crime.

After his graduation from high school, Cheng Zhihan got matriculated by computing department from Qingdao University. Due to the constraints of life within the family, he studied very hard and almost spent all his spare time for doing part-time job to release the workload from his parents offering him financial support. At the second half of the third year study, he had an opportunity to do practical training work at Huawei Cooperation Beijing branch. Because of his hard work and talent, he mastered the process of software development and amazed the project manager. He was invited to the audition at Huawei after his bachelor graduation as well and got employed. [34] After around two years hard working as the first one being at the office, as well as the last one left, his contact with the major projects at the company became more and more. Since 2000, Huawei started to undertake more and more telecommunication core projects from different provinces all around China and he, as one of the brilliant software developer, had to flew around. Sometimes a whole project took more than a quarter. Security guards stopped him several times from entering headquarter made him starting realized several new employees that were not contribute to the company as much as him, had even faster promotion. Injustice and memories on years of hard working started frustrating him.

Soon after, manager informed him the new upcoming project is at Lhasa, a very southwest city in China, which always has a stereotype of underdeveloped place along. The place needs infrastructure for telecommunication, and the project seems would last for a while without regular daily supplements as in a modern city. This made him starts hesitating and the manager promised him similar poor projects would not be arranged to him, instead he will be settled back to Beijing branch and get promoted seriously. In reality, the truth is harsher than what Cheng Zhihan had ever imagined, the whole infrastructure building process lasted for more than fourteen months. However, when he returned back to Beijing, all things was promised would be substituted by another project at somewhere desolate and dull. He was disappointed and made the decision of leaving. Soon, his working experiences, industriousness, and talent found himself another good job at the other telecommunication giant, UTStarcom. [35] However, his arrogance stopped him from merging into the software developing team. Stress from paying loan on extremely high apartment price, paying on high health care fee for

mother, and hopeless on decent promotion at company, set him into self-doubt on career and self-accusation on filial piety.

Cheng Zhihan met a colleague back at Huawei coincidentally on a business trip in January, 2005, and heard China Mobile spent over hundred millions for installing a very decent network security system recently. The colleague was quite proud of his own contribution to the security network and show off the security functions on responding to the network attacks. [35] This made Cheng Zhihan jealous and curious in finding out the exploits from it.

One month later, he remembered the curiosity. Simultaneously, he remembered the project in Lhasa back at Huawei. Due to the technical support team was lack of engineers and him as one of the top leader, set all the security identities for the routers. [35] He was testing to type username and password into the administrative backend of China Mobile Tibet branch. Within short time of exploring in the backend, he surprisingly discovered one database is linking with the voucher database at Beijing branch. He realized this is the one that so-called secure system cost over hundred millions his colleague mentioned. He managed to migrated himself to the database at Beijing branch and gained the highest privilege, along with cracking the password by downloading log files. He started to ridicule the ‘secure system’ secretly. It was quite smooth to get to the data module that contains vouchers. By facing irresistible large number of profits from original passwords, he copied more than a thousand pieces. In fact, he convinced himself that China Mobile has innumerable profits incomes would blind them that ignoring several prepaid vouchers. He attacked the system with the same method for four times. Modifying expiring dates, value, and spending condition on 6,600 vouchers, brought 3.7 million Chinese Yuan loss to China Mobile. [36] Till once he forgot to modify the expiring dates exposed the whole crime to the public.

This is a sad story to the talented engineer for stepping that far, it is also one to such a huge enterprise for having this low-level mistake. 3.7-million-loss probably would not affect such a giant on financial aspect for that much, however, it could be a lot worse if the criminal was a little bit more careful. This whole case reported how a criminal made loss to an enterprise by attacking them internally. It also reflected the situation on large number of enterprises in the market that having low-level flaws and obvious mistakes.

In harsh reality, one exploit within the intranet security policy would lead to very bad penalties or consequences that the business cannot even afford for.

4 LAN ATTACK PROCESS

Since most anti-virus software and firewalls are quite serious on against external invasion, and internal supervision is sometimes relatively loose. Then initializing a series attack would be a lot easier and more silent in certain points. The whole attacking process might be teardown into three main phases. These might not applies to special cases, however, in a sense, it is a conclusion for majorities

4.1 Network Join

In order to initializing an attack internally, first step would be try to break into the network to become one of the regular users. As soon as an Ethernet cable can be reached on a desktop in most office environment, attacker will be a legal intranet member that watching and being watched by the fully functional layer-2 network infrastructure. This provides possibilities to attackers to move to the next step. But there is very little likelihood of that happening since attackers would rather not exposing themselves physically because there might be a chance to get video recorded for future references. Instead, they might prefer to utilize something invisible to break into the network, in this case, Wi-Fi is the brilliant choice.

Wi-Fi signal can be fully detected within the range that signal strength can reach. Even though the self-signal broadcasting function can be turned off, it is still possible to scan it out with certain Wi-Fi cards on a monitoring mode. When a signal is detected, the first analysis would starts running on its cryptography. If WEP encryption method is being used, then an efficient cracking process would ‘calculate’ the password out for joining the network within significant short period of time, sometimes it can be even calculated by seconds. Rather than WEP encryption, network administrators would always love to choose WPA/WPA2 encryption method since they are very familiarize with how fast a WEP can be cracked (sometimes it could also because of WEP needs a specific length of password but WPA/WPA2 accepts any, this might be an advantage of convenience).

WPA/WPA2 would not be easily ‘calculated’ out by an algorithm. However, there still might be three possibilities to crack it. Brute force crack is always one possibility. However, all characters appears in the system including alphabets, numbers, signs are all possibly used by the password, hence innumerable combinations test and time consumption made the brute force crack almost impossible. ‘Dictionary’ is one of the method. An already made ‘guessing’ word list is being used by the attack tool program as a ‘dictionary’. This tool software will try to match up every single phases that stored in the dictionary file with the signal to test out which word is the right ‘guess’. In reality, this method has huge contingency. A huge word list file (sometimes can be several gigabytes plain text file) containing millions of phrases would probably takes days to be tested with the signal without even one match, while another ‘dictionary’ that containing just the right word will works the signal out within seconds. By using this method, it is all rely on the dictionary file whether it includes the ‘needed’ phrase or not. The third possibility is utilizing the WPS function as one exploit. In fact, WPS was invented for convenience purpose. Guests would not need to know the host password to join the host Wi-Fi network with a single click on the ‘rapid link’ button. This function can be utilized by penetration test software for cracking the WPA/WPA2 encryption. Any password, no matter how complicated it is, can be cracked up to eight hours. [37]

4.2 Exploit Discovery

When the hackers are in the intranet, before making any changes or damage to the network infrastructure, they will usually try to make sure what they will do next would not be recorded. In another word, logging system would be the first target hackers want to shut down. This function is typically built into the router or switch. Thus, very few hackers would leave switch and router alone right after they get into the network. If a weak username and password (ex. regular phrases existing in the market ‘root’, ‘admin’, or default settings.) is being used, then the hacker will gain the privilege they want from the very beginning. This would lead to a quite simple and fast attacking process, besides, logs can be wiped after their attacks to make everything seems have not happened ever. Else if the router or switch login system had been modified to reach a relatively secure level, attackers would still not ignore the possibilities that they have the logs being saved to report whom did the attack. In this case, log itself would probably not tell the truth to the administrator because hackers will ‘cheat’ log system. Rather than recording an IP

address on what it did, log system will probably set to record the MAC address on those ones whom touched sensitive system modules. MAC address is the unique fingerprint of one network interface. However, this identity can be modified within attackers' OS. Linux environment will have 3rd party applications that doing the job, while Windows environment will allows user to change it under the property of the network interface. Even though most of the network interface vendors realized it is probably not a good idea to let users to change the MAC address and the modification function within the drivers are usually being removed, it is still possible to 'unlock' this limitation by making small changes to the registry of the Windows system. By then, even though the log will record whom did changes to the system by recording their MAC address, the information they have got are most likely useless.

When the hackers are sure about 'blinding' the network appliances, switches or routers, it is time to make more changes to the intranet. Port scanning is commonly the first choice from hackers to initializing a series attack. As same as a body check before doctors giving advices to patients, port scanning is the 'body check' for victims in IT aspect. In some cases, specific ports that opened might be a lot easier to be utilized as exploits. Also, some ports are very unique to OS, thus the hacker can tell which OS the victim is using in order to prepare for the next step movement. One port scan might returns quite a lot valuable information on the target OS. However, it is still seems as very offensive way of attack.

The port scan can be visualized as a person hover around at a neighborhood that trying to find out which house has its door opening. This will brought cautiousness to the 'people' whom living in the neighborhood. No matter which 'door' is opening, the neighborhood will become an obvious potential victim. By knowing this, victim would call police right away. Reflect back to the IT case, when a port scan is being detected, there would be a chance that active supervising system will notice the intranet administrator. Thus, hackers would rather stay low key than being offensive. That is probably one reason they chose to do a phishing or social engineering attack within intranet.

If the case is the hacker wants to get the victim's username and password on Gmail for example, since usually an email inbox might contains a lot useful personal information that could be utilized for many purposes. First step is the phishing website must be set up as same as possible in comparing with the real one. This will make the victim believe

in the phishing site, where he or she is typing the username and password is in the true Gmail, where he or she wants to or needs to. Certain tool software can download and clone an exact same website as the target one. This is like the ‘people that living in the neighborhood’ want to go to the cinema would not go to the zoo next to it, no matter how similar they look. But if someone can build the exact same looking cinema for them, they cannot tell the difference. Even though there are two cinema look the same, they would not notice since they do not know where the cinema located, but have to ask the taxi to drive them there. Here, the taxi is the Domain Name Server (DNS) in IT field.

Original DNS lookup function are usually built inside the switch or router. It will send users networking requests to the real public DNS to get a result, then return the truth back to the user. For attackers, they will not let the user request being send out to the real DNS. They prefer to make something up and returns it back to the victim. Victim will believe in what they have got returned and starts visiting it. This is like the taxi commander would not tell the taxi driver where the passenger want to go, but lie to them to take the passengers to a wrong address because he got corrupted. In IT section, this attack technique is usually being called poisoning.

When victims are lead to the fake Gmail website, they starts to type in the username and password. In the backend, key-logger will record what they had typed and send it to the specified address (usually the attacker’s network interface). But the fake website that got cloned is nothing functioning but looks same. This might cause victim getting cautious if several times login button click would not return a true login process with the right username and password.

In reality, another software will directs the website from the cloned one to the real DNS server and finally lead it to the real Gmail after the first time login request being received from the user. Thus, a victim might just seeing the website refreshed once after they type in the username and password. They might type it in again because the conjecture of their own mistyping, and the login will truly become successful after the second attempt. Unfortunately, while the webpage refreshing after the first attempt, hackers already got the username and password shown on their screen as plain texts.

4.3 Victim Maintenance

Previous method might be various on diverse situation. Sometimes it could be a social engineering attack that leading the victim give the OS login username and password out. Then the hacker will setup a remote connection between himself and the victim. This illegal network session would be used to doing data transfer or even a node for a botnet that preparing for the next series attack or a massive DDoS attack on others. Then the victim changed into scapegoat. The whole process is quite complicated and limited by many variables. Thus a fully functional victim is very valuable to the hacker. They definitely would not like to repeat the same process of series attack again, neither want to forget the victim as they might brought more benefits. Thus, hackers would try to set up one invisible interface on the victim for themselves to connect to in the future, this is also known as a backdoor. Reverse connection might be managed to implement with payloads. Multiple algorithm are utilized to hide the typical characteristics of the back-door virus from being detected, reported, and killed by an anti-virus software on the victim's OS. This process is very much like setting up a VPN connection between victim and hacker. Thus, the maintenance process are also being called as tunneling. A reverse connection virus are being running on the victims OS, this will significantly consume quite a lot computing resource. If the victims know a little bit about the task management on Windows system, there would be a chance that they can investigate and find out which process is the most power consuming one and terminate it. Then the hacker would not like to see the tunneling process being interrupted by the victim. Hence, they will migrate the virus process from itself to a system process so the victim cannot easily ends it unless they turn the whole system off. With the setting of self-startup while OS booting up, the victim would be under supervising of the hacker as soon as they have an internet connection.

In fact, any of the most common attack methods mentioned in the previous chapter needs the precondition, which is the loophole. This is the same as exploit discovery within the attack process. Also, when hackers want to maintain the victims, they might need to send payloads containing virus and malicious codes. These are all similarities between any of the attacking methods or processes. Thus, the whole LAN attacking process being studied in this chapter is a very nice guidance for the laboratory design in the next step.

5 SERIES ATTACK SIMULATION

All the attacking methods and process are introduced in the previous chapter. In order to experience a series attack, one lab environment will be setup. As for saving physical appliance source and efficiency, individual OS within the network will be created under system virtualization freeware. Additionally, expect for individual wireless accessing point would be physically configured, routers and switches will be setup by GNS3. The simulation assume hacker needs to get significant email login information from the victim without let him being perceive. Victim is already known as working in a closed office. The whole attack process would be implemented in the next few breakdown phases.

Additionally, GNS3 is one network appliance emulator, mainly emulate Cisco products. As soon as the users has legal copies of IOS (cisco product system image), they can use GNS3 to emulate the appliance that almost have every feature a physical one has. Due to GNS3 program has all versions for main three OS (Windows, Linux, and Mac OS), it is a cross platform network appliance emulator being widely used for education and laboratory environment. Other open source router emulators are existing in the market as well (ex. BSD router project can turns one Linux based PC into router).s

5.1 Creep into the environment

Merely have Ethernet connections is not enough to simulate a relatively realistic environment. Hence, Wi-Fi signal should be considered. As well, a 64-bit/128-bit WEP encryption is old fashioned, most enterprises already realized WPA/WPA2 is a lot better and securer. The environment setup would simply assume the wireless network left the WPS function on, in order to give convenience to the potential guests whom would come for visiting.

Internet Service Provider (ISP) will pass the connection to the wireless accessing point (AP), then one switch will handle all the traffics for staff's desktops in the office. The hacker will use a laptop with monitoring mode compatible wireless card that sneaking behind the wall. The main target is to crack the Wi-Fi password to join-in without noticing anyone else in the victim environment (FIGURE 8 as a topology reference).

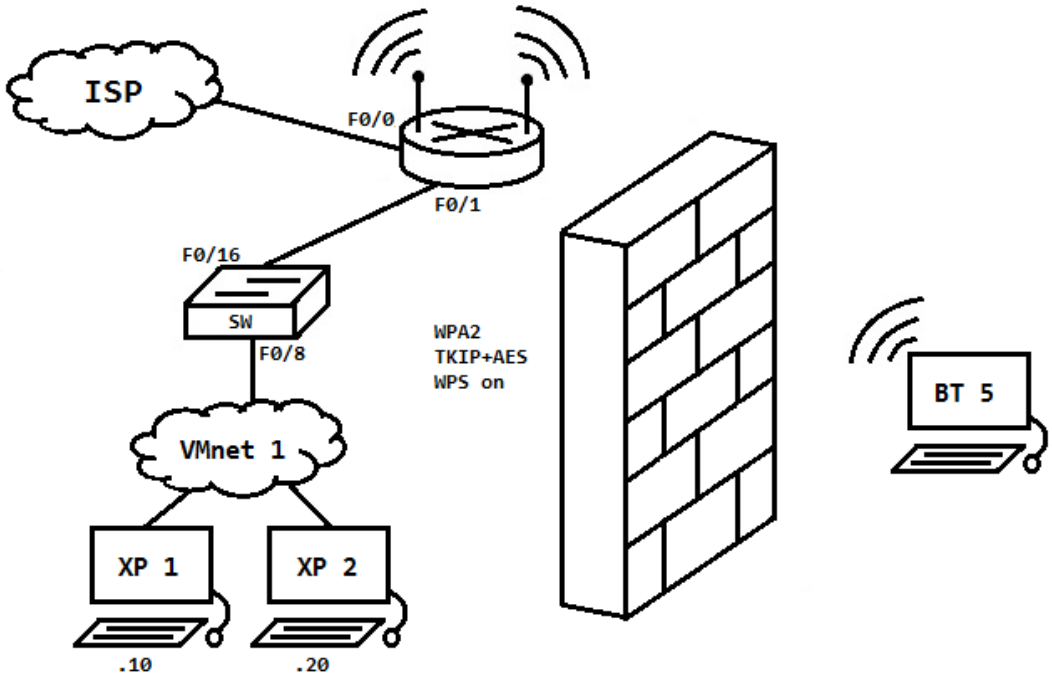

FIGURE 8. Crack Wi-Fi Password through WPS PIN

As mentioned in the previous chapters, hacker would not like to have the wireless AP record down their behavior. Then the first thing to consider is the stealth. Log system might write down whom did authentication and data negotiation with it. Thus, even though there might be a chance to wipe all logs after breaking into the wireless system, it is still less risk to make changes to the hacker himself from the beginning. For further penetration test convenience, the host environment was chose as using BackTrack 5 (Linux). Without having the right MAC address, it is almost impossible to trace back with the vendor headers. Within Linux environment, one small application 'mac-changer' will do the job (FIGURE 9).

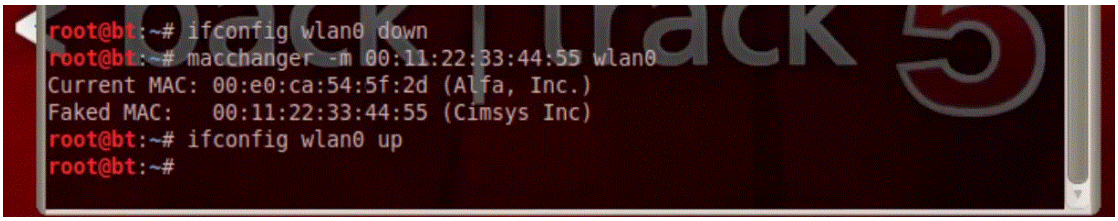

FIGURE 9. Change wireless NIC MAC address with macchanger

Aircrack is a tool set that containing add-ons for turn compatible wireless cards into monitor mode, data packets capture, records analysis. The process is quite complicated and all manual. One application for Linux called 'minidwep' utilize all tools come along with Aircrack package and GUI made the usage quite straight forward (30513 version

is required since any other version before 21026 does not has function to crack a WPS PIN-code). Minidwep provides Wi-Fi signal scanning and analysis, filter function would speed the scanning process up if hacker knows which specific channel the signal is operating on. At the end of the signal lists, it would automatically list up whom is compatible with WPS exploits (FIGURE 10). 'Reaver' is the right tool for calculating PIN codes with WPS function. Technically any number from zero to nine would be possible to appear within the PIN code (usually eight digits). This means the possible combinations are 10^8, which is a hundred million. Such huge number will consume a lot time to test the right PIN out. However, reaver has its own algorithm, besides, there will be certain characteristics for the PINs from vendor to vendor. This feature considerably reduced the period for PIN matching.

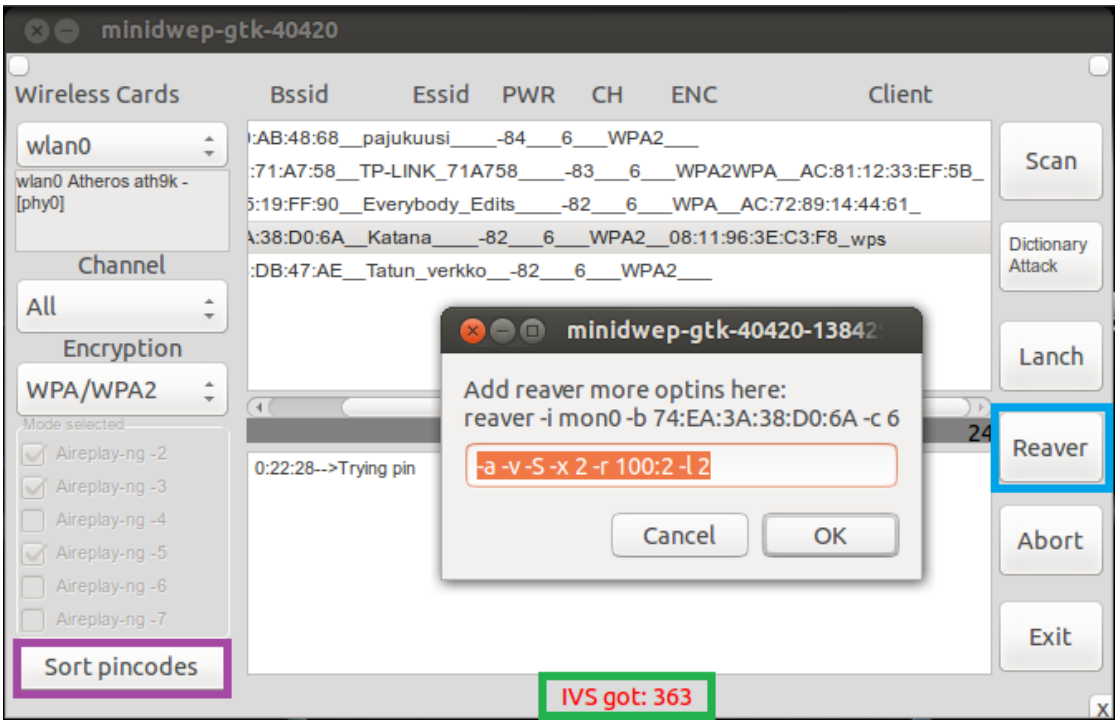

FIGURE 10. Minidwep-gtk-40420

When the right signal with WPS in the list is selected, there will be a 'reaver' button appears on the right hand side (FIGURE 10 within the blue box). Clicking on that will brings up a window asking command suffix, all choice can be found within the terminal with the suffix '—help' to reaver. Also the PIN permutations and combinations can be also modified on the left bottom corner (FIGURE 10 within the purple box). When everything is set up and confirmed, minidwep will call up reaver add-on and starts to associate with the AP, during this process, minidwep will also capture packets that contains useful data (FIGURE 10 within the green box). When it has effective handshakes

with AP, reaver will starts its PIN-testing process. With this simulation case it took three and half hours to calculate out the right PIN. A popup windows will show the PIN code and password to the hacker. Till then, hacker is here at intranet without noticing anyone in the victim office to press the WPS button to let him connects legally.

5.2 Familiarize with the environment

When the hacker is here inside the network, he would probably love to walk around to see whose OS has loopholes that can be directly utilized. This breaks into two categories, network scanning and exploit discovery. To do a complete intranet scan would be a time consuming work. It also depending on which tool is using and which information are gathering. Specific command suffix will refine the scanning process and save a lot unnecessary time wasting. 'Genlist' is one of the fast scan tool will returns the simple IP address that are active on the subnet (FIGURE 11 left). With the result that got from 'genlist', 'nmap' will do analysis on specific target IP. 'Nmap' is one of the best network scanning tool exists due to its functionality. In fact, there is no need to use 'genlist' besides 'nmap'. It can discover active hosts as well. Additionally, 'nmap' will detects the target's active service or version, OS. It can even do network traceroute and become one Nmap Scripting Engine. In this case, the hacker will do a fast scan on the specific target and gathering the target information (FIGURE 11 right).

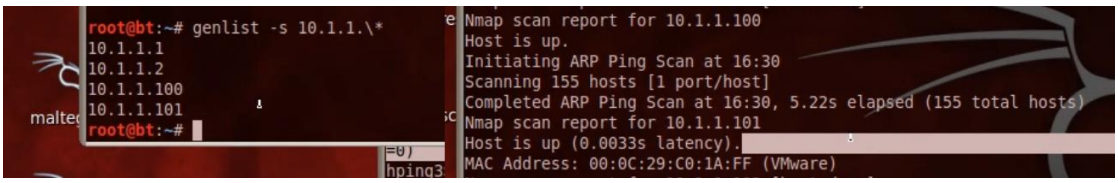

FIGURE 11. Genlist & Nmap

Information will be get together after s network scan. Nmap will utilize the OS finger print and certain opening port to make a guess on the target OS. In this case, all intranet users are using Windows OS except for the attacker. Penetration test would be a lot easier if there is any exploit that can be directly utilized to give hacker a relatively high privilege for entering the victim OS. The tool with GUI would be easier to manage a massive network. Even though this case is not as complicated as a real enterprise environment, 'Nessus' would still be the best choice. This is a cross platform exploit/loophole scanning tool. It can be used as an analyzing tool for intranet security status scan,

either way, it can be a good exploits discovery tool for hackers. Setting process is quite straight forward due to a tidy friend GUI (FIGURE 12 upper left). Then the scan will take a short while to do an analysis on the target subnet. After the whole process, 'Nessus' will returns a list containing the active targets and their loopholes (FIGURE 12 upper right). Every single exploits can be viewed in details for further attacks prepares (FIGURE 12 lower left). It also supports users to do customization on scanning policies (FIGURE 12 lower right).

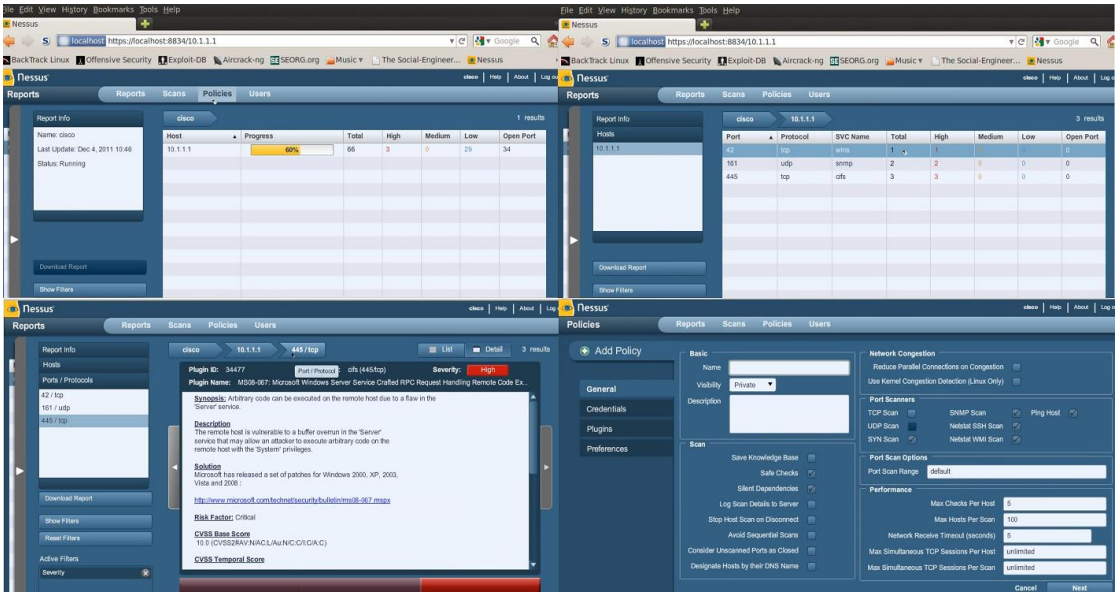

FIGURE 12. Nessus

When exploits are discovered, there are simply two ways to go. Hacker can either go with an individual loophole, which if he is familiar with the specific one. As well, there is another tool for doing an automatic exploits test and penetration, 'autopwn'.

This is one module from a famous penetration test toolkit 'Metasploit Framework' (MSF). Including 'nmap' and many other network scanning, information gathering, exploit discovering modules are built into MSF, 'autopwn' is one from the loophole discovering category. However, due to its high automation and ease of use, MSF official team had many problems, warnings, and even lawsuits that brought by this 'autopwn' module. Thus the official package removed it. Fortunately, it is still possible to bundle it back in owing to the modularized design on the main framework.

5.3 Spoof & Fabricate the environment

Exploits are easily scanned out due to the simulation environment was set up on virtual machine without doing security OS updates. In a realistic case, OS running heavily without automatic updates would rarely happens. Phishing is one of the most silent way to steal credentials without noticing victims easily. Thus, hacker would like to set up a fake Gmail web interface to wait on the victim step into the trap himself. However, all the traffics generated from the victim that heading to Internet will directly going to the true destination through gateway. Hacker need to become a middle man between gateway and the end victim. There are two similar methods for achieving the goal, Unknown Unicast Flooding and ARP Spoofing. Both are utilizing the operation principle on data link layer.

Since the appliance need to know which MAC address does the packets came from and going to, it 'registers' the MAC address in its MAC address table. However, the list has limited space. If it is full, the appliance would not register new MAC address anymore. By then, if a new data packet come to the appliance, it would not understand the destination header. Then it will floods the packet to everyone on the intranet to see if there is a 'right' receiver. This attack method is trying to generate heavy load of useless MAC address to fill the table up and then listen on the NIC so it could recognized any sensitive packets it is looking for when the appliance is flooding them. There is one small tool under BackTrack 5 called 'macof' (FIGURE 13 left). It basically generates junk MAC addresses and try to let every single one registered in the appliance's MAC table (FIGURE 13 right).

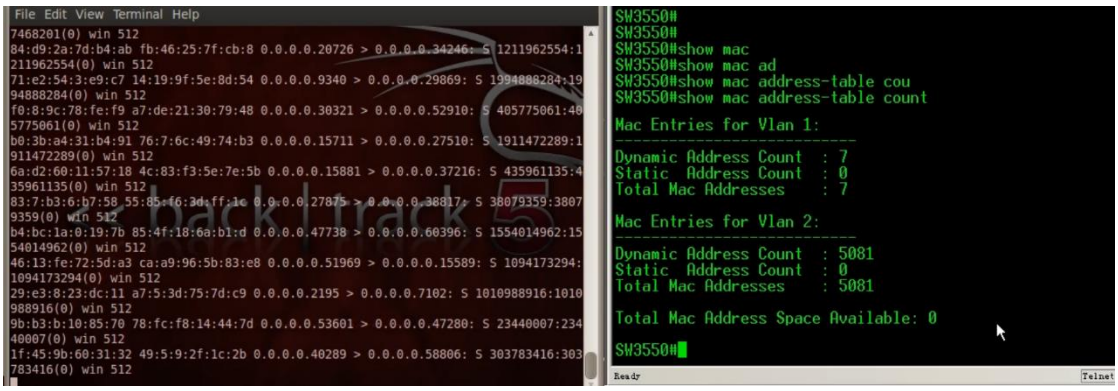

FIGURE 13. Macof filling appliance MAC address table

The other method is ARP Spoofing on the appliance. As same as previous method, appliance should has its own table that records the true address where the packets came and going to. This attack is trying to poison the appliance so the hacker's OS can act as one hop between appliance and victim. Assume appliance address is A, the victim one is B, and the hacker's one is C. Originally, communication between A and B should flows quite normal, C cannot capture any useful information. With the attack, first C will send an ARP reply to A that tells him the B address is indeed C. Then it will also tell B that the address of A is actually C as well. After these two sides believes in what C told them, C needs to start the routing function to make the packets that flow towards him eventually flow to where it supposed to go. In this case, all packets that should going through the appliance directly, will pass through hacker's OS first. This made any network sniffing tool like WireShark is able to capture sensitive packets. 'Arpspoof' and 'ettercap' from BackTrack 5 can all do the job, while 'ettercap' is more functional.

When data will flow through hacker, he would like to be more offensive instead of just waiting for the usernames and passwords. If an exact same Gmail website is cloned and hosted by the hacker, and the victim could be misled to the hackers fake Gmail, it would be a lot faster to get the credentials. To lead the victim to the hacker's fake website instead of the real one, DNS is the key point. Visiting wish request to the destination IP address needs to be translated through a DNS from plain text domain. Usually DNS is the responsibility of the appliance. Hacker need to take the job over and point the certain IP translation to himself so that every time victim asks to visit the certain webpage will be misled to hacker. 'Ettercap' can do not only ARP Spoofing, but also DNS cheat. There is one file under the installation folder controls the DNS 'translation rule', in the simulation case, it is '/usr/share/ettercap/etter.dns' (FIGURE 14 left within orange box). After the 'new rule' is set, activate the DNS spoof function under 'ettercap' and verify it with a ping command (FIGURE 14 middle and right).

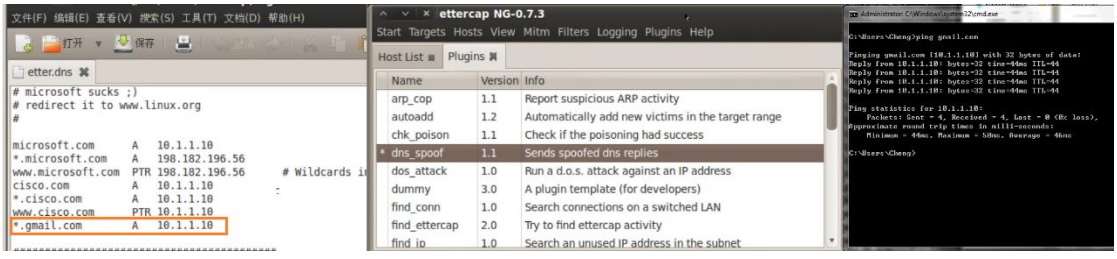

FIGURE 14. Ettercap DNS Spoof

Now fake DNS has been set up and the next step is to clone one Gmail webpage make the trap looks exactly the same as the real one. ‘Social-Engineering Toolkit’ (SET) is a full package that comes with a lot functional add-ons that all related to social engineering attack. Start the SET and choose from the menu: ‘1) Social-Engineering Attacks’, ‘2) Website Attack Vectors’, ‘3) Credential Harvester Attack Method’, and ‘2) Site Cloner’. Then type in the webpage that want to clone from, in this case, it is ‘https://gmail.com’ (FIGURE 15 left within blue box). After it finished the cloning process, it would returns a notice that inform the hacker this SET will wait on port 80 to show sensitive information (FIGURE 15 left within green box). As soon as any victim that get onto Gmail and trying to login, there will be a message that tells the credentials it captured on SET (FIGURE 15 right).

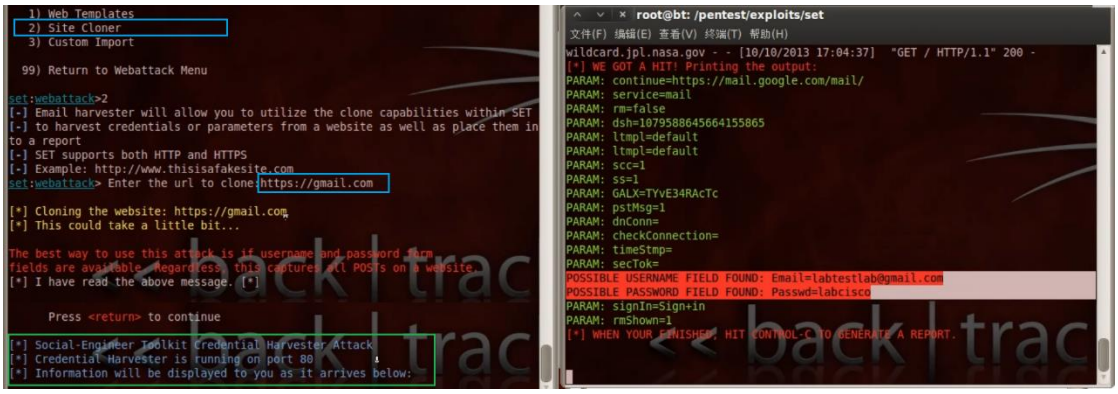

FIGURE 15. SET Clone Gmail & Capture Sensitive Info

After capture the credentials, fake DNS will pass the job back to the real one and directs the original request to the real Gmail. When the second time that victim type the login information, he will log into the Gmail account. However, on the other side, hacker already achieve the goal and able to reads any email with the right username and password. There are several other payloads this SET could generate. Some of them might needs Java script so it would only works when victims did not pay enough attention to the pop up Java script authentication request window and admitted. However, Java based attacks will automatically generate a Trojan process in the target OS (for Windows case) and set itself as a startup running program. Hacker can also migrate the remote session to system original ones that has administrator privilege (ex. Explorer.exe, etc.). Key logger, screen snap shots, integrated camera utilization are all available. All data are exposed under the hackers destroy wish. Evident, a small exploit existing in the intranet would brought a series problems.

It is noteworthy that any Linux based OS might have the possibilities to initiate a network spoof attack, this including mobile devices (ex. Cellphone, tablets). Laptop was one of the most popular penetration tool was because of its extensionality, even though it does not has one monitor mode compatible wireless card, it is still possible to attach an external USB or ExpressCard one. As well, OS that operates on a laptop can be diverse, especially due to virtualization, attackers can shift to any platform as they need instantly. Mobile phone is a lot handier and sneakier than a laptop to be carried around to achieve the simple goal. A handful of the cellphones has a monitor mode compatible Wi-Fi card, yet N900 from Nokia is one of them. With the card, it is possible to operate the Aircrack package or many other similar wireless penetration packages, even Metasploit Framework on its Linux based OS Maemo (FIGURE 16), which brought great possibilities to the hackers to initiate various attacks.

FIGURE 16. Aircrack, Reaver, Metasploit Framework on N900

On the other hand, network spoof like ARP spoofing become more and easier on a cellphone as soon as it is in an intranet. This does not requires any compatible wireless NIC to do the job. Any Android based cellphone could run those packages. One representative is Network Spoofer (FIGURE 17 left three). This tool allows end user poison the wireless router to blind the original DNS. No matter which website the other users whom connected to the same router wanted to explorer, it will directs them to a pre-specified webpage. This could be a real website on Internet or either could be one that someone hosts for a shady purpose. In fact, Android as one brilliant member from Linux family, is more powerful than Maemo. As soon as the hardware is powerful enough, Android can run as heavy load as a regular Linux system. BackTrack 5 has one special version that suites the ARM architecture based cellphones (FIGURE 17 right). Android can do simple virtualizations sometimes as well, this means to migrate Windows OS to Android is not a dream anymore.

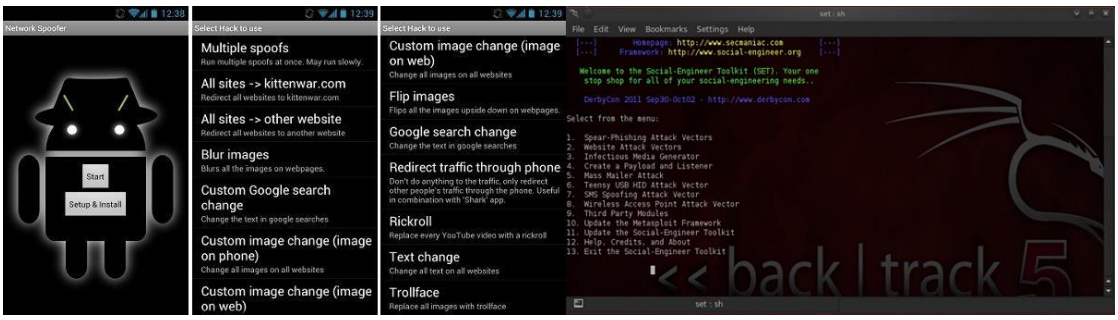

FIGURE 17. Network Spoofer & BackTrack 5 on Android

Thus a handy device in someone's pocket would become a hacker tool easily and instantly. This made the physical security check harder and harder for the potential victims. Network security issue became more and more severe, tiny negligence would brought huge data or financial loss.

6 CONCLUSION

Among this whole study on vulnerabilities affecting intranet security, several common attacking methods was researched to form theoretical background nodes. One relatively heavy case significantly gave a caution out for the loss that brought by negligence on intranet security. Common LAN attacking process reflected the usual way that attackers would implement by utilizing and combining typical attacking methods. These studies firmly outlined part of the networking attack situation in the near past. Practical laboratory strongly helped to understand the attacking process, and in a sense, it also helped to pay more attention to the similar vulnerabilities in the practice future.

While, the real enterprise environment is definitely more complicated than the laboratory had been designed here. Network scale, configurations, physical situation, IT supports are all instances of many variables and limitations for the feasibility of the design in a real life case. This thesis study is one decent example on penetration possibilities on loopholes from intranet security, even though it cannot be fully assess as featured representative in real networking environment. Absorbing experiences from it would help to prevent similar attacks and develop further securer network architectures.

Either Internet or Intranet situation is changing time to time, diverse attacks are shifting themselves more simultaneously. Traditional offline attacking methods are fading and revolute themselves into a streaming live mode. Ways are sneakier and technologies are

going to make the attacks consume less and less computing resources. Space that left for end users that exposed under the threats are smaller and smaller. It is almost impossible to absolutely avoid attacks, only being careful and knowing more IT related tips would probably reduce the chance to get invaded. Wireless signals would possibly became one of the most vulnerable gateway to occupy others' network.

Since more and more industries starts relying on information technology, patents, secrets, or even valuable human resources are all available in the private databases. Immeasurable loss could happens if any exploits or flaw in the system could be utilized by a commercial spy with IT skills. Thus, individuals and enterprises would probably love to pay as much attention that paying to against external attacks as to internal ones. Importance of Intranet security is easily to be overlooked, yet should be easily armored up likewise.

BIBLIOGRAPHY

[1] **Trojan Horses** by ThinkQuest
Available in www-format
<URL: http://library.thinkquest.org/08aug/01692/trojan.html >

[2] **PC-Write** by Wikipedia [referred Sep 2013]
Available in www-format
<URL: http://en.wikipedia.org/wiki/PC-Write >

[3] **History of the internet: a chronology, 1843 to the present** by Christos J. P. Mos chovitis [referred 1999]
Available in book-format
<URL: http://www.amazon.com/exec/obidos/ASIN/1576071189/isbncheckcom-20>

[4] **Flame virus may have 'partners'** by NewEurope [referred 19 Sep 2012]
Available in www-foramt
<URL: http://www.neurope.eu/article/flame-virus-may-have-partners >

[5] **Flame: Massive cyber-attack discovered, researchers say** by BBC [referred 28 May 2012]
Available in www-format
<URL: http://www.bbc.co.uk/news/technology-18238326>

[6] **The Flame: Questions and Answers** by Aleks from Kaspersky Lab Expert [referred 28 May 2012]
Available in www-format
<URL: https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers >

[7] **'Panda light incense' virus manually cleaning tutorial** by Xdowns.com [referred 15 Jan 2007]
Available in www-format
<URL: http://www.xdowns.com/article/170/article_696.html >

[8] **'Panda' is not cute, 'light incense' everywhere** by Morning [referred 20 Dec 2012]
Available in www-format (in Chinese)
<URL: http://morning.scol.com.cn/2007/01/22/20070122451304447211 4.htm >

[9] **The Morris Internet Worm** by Charles Schmidt and Tom Darby [referred Jul 2011]
Available in www-format
<URL: http://www.snowplow.org/tom/worm/worm.html >

[10] **The Froehlich/Kent Encyclopedia of Telecommunications** by CERT/CC [referred 1997]
Available in book-format
< Vol. 15. Marcel Dekker, New York, 1997, Page 231-255 >

[11] **United States v. Morris** by Dressler, J. [referred 2007]

Available in book-format
<Criminal Law. St. Paul, MN: Thomson/West. ISBN 978-0-314-17719-3.>

[12] **Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'** by Kim Zetter from Wired [referred 25 Mar 2013]
Available in www-format
<URL: http://www.wired.com/threatlevel/2013/03/stuxnet-act-of-force >

[13] **W32.Stuxnet Dossier** by Symantec [referred Feb 2011]
Available in pdf-format
<URL: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf Figure3 Geographic Distribution of Infections on Page. 6>
[14] **Stuxnet worm slithers into China, heralds alien invasion** by John Leyden [referred 1 Oct 2010]
Available in www-format
<URL: http://www.theregister.co.uk/2010/10/01/stuxnet_china_analysis >

[15] **Computer Virus Alert: Beware of Stuxnet virus spread through USB drive** by The Central People's Government of the People's Republic of China [referred 27 Sep 2010]
Available in www-format in Chinese
<URL: http://www.gov.cn/fwxx/kp/2010-09/27/content_1710601.htm >

[16] **Siemens: Stuxnet worm hit industrial systems** by Robert McMillan [referred 14 Sep 2010]
Available in www-format
<URL: http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142 >

[17] **Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target** by Kim Zetter from Wired [referred 23 Sep 2010]
Available in www-format
<URL: http://www.wired.com/threatlevel/2010/09/stuxnet >

[18] **Kaspersky Lab provides its insights on Stuxnet worm** by Kaspersky [referred 24 Sep 2010]
Available in www-format
<URL: http://www.kaspersky.com/news?id=207576183 >

[19] **Iran 'first victim of cyberwar'** by The Scotsman [referred 15 Sep 2010]
Available in www-format
<URL: http://www.scotsman.com/news/iran-first-victim-of-cyberwar-1-811906 >

[20] **Iran – First Victim Of Cyberwar** by William Maclean from Pakalert [referred 26 Sep 2010]
Available in www-format
<URL: http://www.pakalertpress.com/2010/09/26/iran-first-victim-of-cyberwar >

[21] **Warning from 'Stuxnet'** by Zhenglong Wu from Sina [referred 10 Feb 2011]
Available in www-format in Chinese

<URL: http://news.sina.com.cn/w/2011-02-10/063021931038.shtml >

[22] **About DDoS attacks** by BlackLotus
Available in www-format
<URL: http://www.blacklotus.net/learn/about-ddos-attacks >

[23] **Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks** by Fei Xing & Wenye Wang from North Carolina State University [referred 23 Apr 2012]
Available in pdf-format
<URL: http://www.ece.ncsu.edu/netwis/papers/06xw-milcom.pdf >

[24] **Trinity distributed denial of service tool (IRC_Trinity)** by ISS.NET [referred Aug 2012]
Available in www-format
<URL: http://www.iss.net/security_center/reference/vuln/IRC_Trinity.htm >

[25] **System Security: A Hacker's Perspective** by Felix, Jerry and Hauck, Chris [referred Sep 1987]
Available in book-format
< 1987 Interex Proceedings 8: 6. >

[26] **Phishing and Spamming via IM (SPIM)** by Koon Yaw Tan [referred 2 Dec 2006]
Available in www-format
<URL: http://isc.sans.edu/diary/Phishing+and+Spaming+via+IM+%28SPIM%29/1905 >

[27] **Phishing** by Word Spy [referred 28 Sep 2006]
Available in www-format
<URL: http://www.wordspy.com/words/phishing.asp >

[28] **GP4.3 - Growth and Fraud — Case #3 – Phishing** by Financial Cryptography [referred 30 Dec 2005]
Available in www-format
<URL: https://financialcryptography.com/mt/archives/000609.html >

[29] **Fake subpoenas harpoon 2,100 corporate fat cats, From phishing to whaling** by Dan Goodin from The Register [referred 16 Apr 2008]
Available in www-format
<URL: http://www.theregister.co.uk/2008/04/16/whaling_expedition_continues >

[30] **Phishers Snare Victims With VoIP** by Gonsalves, Antone from Techweb [25 Apr 2006]
Available in www-format
<URL: http://www.techweb.com/wire/security/186701001 >

[31] **Online Fraud And The Financial Phishing Scams: Brand Abuse May Be Coming To A Blog Near You** by RobinGood [referred 1 Jul 2009]
Available in www-format
<URL: http://www.masternewmedia.org/online-fraud-and-the-financial-phishing-scams-brand-abuse >

[32] **Identity thieves take advantage of VoIP** by Silicon.com [21 Mar 2005]
Available in www-format
<URL: http://www.silicon.com/research/specialreports/voip/0,3800004463,39128854,00.htm >

[33] **More Pie Charts & Fingerprinting (DDoS & Security Reports)** by Arbor Networks [referred 14 Apr 2008]
Available in www-format
<URL: http://www.arbornetworks.com/asert/2006/04/more-pie-charts-fingerprinting >

[34] **Prepaid Voucher Pin-code got hacked, Frustrated Engineer Devoured 3.7 million from China Mobile** by CnFamily.com [5th Publish, 2006]
Available in www-format
<URL: http://shang.cnfamily.com/200605/ca30317.htm >

[35] **Contest on the security of the database, engineer hacker dug 3.7 million from China Mobile** by GlobalTracks [referred 6 May 2006]
Available in www-format
<URL: http://wyliang80.blog.sohu.com/2816315.html >

[36] **Talented Engineer turned into hacker made grate loss to China Mobile** by TeleAsiaPacific.org [referred Aug 2006]
Available in www-format
<URL: http://newschina.teleasiapacific.org/2006/08/7369132876.html >

[37] **Brute forcing Wi-Fi Protected Setup** by Reaver-WPS Project [Dec 2011]
Available in pdf-format
<URL: http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf >