

PACKET SAGA, USING STRATEGIC HACKING TO TERRORIZE COMMERCIAL AND GOVERNMENTAL ENTITIES ON THE INTERNET

Khaled M. A. Nassar knassar@nile-online.net

Wael A. Ali wali@nile-online.net

The Egyptian Company for Internet and Digital Infrastructure, Nile Online, Egypt.

Abstract: This research paper objective is to show the massive impact that hostile action like electronic terrorism has on the internet. The paper begins by explaining some of the actors in such action and their motives. Then the paper will present, step by step, the evolution from a simple hacking technique to a strategic technique as a sample of how effective and destructive hacking could be. The paper presents a strategic hacking framework that was integrated and experienced by the research team. This framework shows how information could be used to terrorize the network operations of a company. Moreover, the effect may extend to compromise the organizations business outside its cyber borders. The threat may extend in some cases where national security is compromised. Then the paper will present simple scenarios for implementing such framework in attacking organizations that are different in nature (one is governmental and the other is commercial) as well as the motive that makes someone attacks them. The scenarios will show the impact on these organizations. Afterwards the paper will be concluded and an overview of types of counter measure will take place. Finally the recommendations for enhancing research and development in the field of computer security and increasing the awareness of the community in such field will be presented.

Keywords: E-terrorism, Commercial, Governmental network.

1. INTRODUCTION

The Internet has become one of the largest investments in modern history. The Cyberspace serves many aspects of our modern life. These services include e-government, e-market, and scientific services. The growth rate of the internet is humongous but unfortunately the internet was not designed to secure such a large interactive network of interests. The threats that compromise the internet users, home users as well as organizations, varies in popularity, impact and solutions. However, no entity on the internet is one hundred percent secured.

Electronic terrorism was debated in the past years. But it was not until the 11th of September crisis that it drew huge attention to the possibility of its existence, its motives and counter measures. The purpose of this paper is to discuss the idea of e-terrorism with emphasis on how it takes place, the motives of the e-terrorists, the technical milestones in performing such an action, the possible counter measures, and a theoretical proof of concept of E-terrorism destructive impact on the cyber society.

The paper is divided into four main sections. The first section briefly goes through the various services that the internet provides, the actors of the internet warfare and their motives. The second section concentrates on the intrusion techniques and how simple techniques could propagate to cause terror on the internet. The third section is a proof of concept that intruders can terrorize Internet entities. This section will present scenarios for terrorizing both governmental and business electronic entities to conclude the research assumptions. The fourth section is a short one that will go through the countermeasures as a preface for the recommendations following it.

2. ACTORS, NETWORKS, AND MOTIVES

In this section we will review some of the variant types of networks that could be recognized on the internet. After this brief review we will explain the different reasons that could motivate an intruder to attack a network. And to complete the vision a definition of the actors who play roles in these events will take place as the last part of this section.

2.1. Electronic Entities/Services

Many organizations use the internet to upgrade their services. The internet itself is roughly a communication network. But a researcher could recognize some distinguished domains of services' networks built upon it.

Governmental networks, Banks or monetary networks, scientific networks, and other business networks appear to be most significant. Another important but different in nature networks are the social networks. All these networks can be hacked and all need security measures to decrease the risks that face them.

2.2. Motives

Networks are penetrated for many reasons. An attacker could find a couple of reasons to attack a target. For example, the attacker would want to satisfy his or her ego and talk about an operation he or she performed in public or private groups to gain the respect or admiration of other internet users. But, when he or she attacks it will be the network of an organization of an enemy company or a company that refused his or her employment application.

2.2.1. Hacktivism

Hacktivism can probably best be described as the hacking for political reasons. It's obviously a contraction of hack and activism. The theory is that some hacker will use his skills to forward a political agenda, possibly breaking the law in the process, but it will be justified because of the political cause. An example might be a Web-page defacement of some will-selected site with related message. It might be planning a virus at some company or organization that is viewed as evil. [Ryan, 2000]

2.2.2. Hacker-Nerd Connection

Probably the most widely acknowledged reason for hacking. It seems that a very large number of the hackers out there want some amount of recognition for their work. You can call it a desire for fame, you can call it personal brand building, you can call it trying to be "elite", or even the oft-cited "bragging in a chat room". [Ryan, 2000]

2.2.3. For Knowledge

In a world where a person is recognized by how much he knows it's not weird that knowledge and quest becomes a very popular. In almost every hacking website or any famous hacker lair there is a question among its FAQ section called "will you teach me how to hack?" This question is often replied to by that the newbie should read, read, and read till he is good enough to ask new questions. We could imagine how huge the number of Newbies surfing the net trying tool, script, and exploits trying to understand. Penetrating a system is an attractive thing to do for most enthusiastic

technology involved people; it implies good knowledge of the penetrated system which is an appreciated quality in the information age, at least for some.

2.2.4. Industrial Espionage

The difference between competitive intelligence and industrial espionage, for example, is significant. By definition, industrial espionage refers to illegal activities - which range everywhere from outright theft to bribery and everywhere in between. Conversely, competitive intelligence collection is governed for the most part by adherence to corporate and professional ethics which preclude the use of illegal means to obtain information.”[Nolan, 1996]

2.2.5. E-Terrorism

How serious is the danger of Internet-based terrorism? [Fisher,2002] Since Sept 11, terrorism is head news, and the computer world is waiting for the e-terrorism. [Winkler, 2001]

"As soon as someone uses the term e-terrorism they begin to lose credibility with me," says Graham Ingram, general manager for Internet security watch-dog AusCERT. "The whole idea of terrorism is to do something that creates terror. You need the physical realization of violence, and there is very little terror inspired by bits and bytes". "You might have a terrorist act which involves violence and death, and somehow interrupt the 000 emergency numbers so that the authorities couldn't respond as effectively." Ingram says. Kim Valois, security service director at IT integrator CSC not agree with Ingram. He said that e-terrorism can include the use of information systems to support terrorism.

"Any disruptions to information systems that are in public use, like banking or transport, any use of such systems to disrupt, undermine or cause damage in some way -- attacks against the power supply or the banking system -- these are all part of e-terrorism." Valois says. "However, some groups are more likely to use the Internet for information dissemination or fundraising activities."

Although internet can be used by terrorist, the occurrence of e-terrorism is still low. and this because terrorist usually need to make fear and visual image fear. If we mention Oklahoma City, with the images of buildings blown away come to mind. With Pan Am flight 103, the image of a side of a 747 comes to mind. TWA flight 847 created the image of a terrorist in a mask holding a gun to the head of a pilot. There is Samples for e-terrorism like crash of the AT&T telephone network in 1991, the power outage in the

Pacific Northwest in 1998, the denial of service attacks in 2000, the Chinese "info war" and the Code Red and Nimda worms of 2001. Consider what the following mean to you personally: Code Red and anthrax. Clearly, anthrax creates a whole different level of fear. Traditional terrorists appreciate the Internet and the resources that it offers. It provides a ready way to exchange information. So the traditional terrorist won't destroy internet. But the only exception is computer attack against companies supporting military attacks.

But there is another threat from nontraditional terrorist. They are Groups who want to damage technology or create negative effects on companies for specific reasons. For example, if someone could take down McDonald's shipping computers that are involved in getting stock to McDonald's restaurants, they could cause damage to its revenue. Any company with an international presence is a possible target for one obscure reason or another. General Marsh, the head of the now disbanded President's Commission on Critical Infrastructure Protection, declared that "banks lose billions of dollars a year to electronic thefts. Statistics about computer crimes continue to climb". [Winkler, 2001]

This all clears the danger of the new terrorism "E-terrorism" which many government officials and terrorism experts consider a serious threat to national security with the potential for causing mass confusion and loss of life. The Bush administration confirmed that it will spend \$10 million to launch a newly intensive war against cyber-terrorism, "Cyberspace," said one Bush administration official "is our next battlefield. And the president has concurred that we need to be better prepared for it." President Bush will appoint Richard Clarke, the longtime coordinator of security, infrastructure protection and counter-terrorism for the National Security Council, to the position of special advisor to the president for cyberspace security. Retired U.S. Army Gen. Wayne Downing will be appointed deputy national security advisor and "national director for combating terrorism," administration officials said. [Thomas, 2001]

2.3. Actors

In this section we will go through the different actors in the information warfare in the cyberspace. Different opinions are discussed here some opinions clearly oppose each others especially when it comes to the hackers and crackers which will be shown in the following review.

2.3.1.Hackers

A hacker is a term that means a clever programmer and someone who knows a lot about programmable systems and how to increase their

capabilities. Originally a hacker was someone who makes furniture with an axe. But in the new hacker's dictionary, which is also referred to as "the hacker's jargon", Eric Raymond (compiler and maintainer of the jargon) lists some of the hacker's characteristics. The first is that hackers enjoy learning the details of programming languages and programmable systems. The second is that they really enjoy programming, in other words programming is a hobby rather than a job to perform or theoretical issue to talk about. The hacker's ability to pick up programming quickly is considered another characteristic. Another characteristic is that they are experts in a particular language or system as in Unix hacker or C++ hacker. One of their most important characteristics that could not be described better than Raymond's word as he describes a hacker "One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations" [Raymond, 2000]. Finally they appreciate other hackers' hacks. [Raymond, 2000]

2.3.2. Crackers

The cracker is the one who penetrates systems and perform malicious actions like destroying data, denying the service of some sites, or stealing data. Raymond says that they often call themselves hackers but their involvement in vandal actions is what differentiates them from hackers. [Raymond, 2000] Moreover, a cracker could turn into a hacker in advanced phase of his or her cyber life. After outgrowing the desire to crack and penetrate systems crackers understand the real meaning of hacking and stick to the hackers' ethics. [Raymond, 2000]

2.3.3. White Hats

As described by "whatis.com" white hats are hackers who search for vulnerable systems and report these vulnerabilities to the owners of those systems. They don't oppose a threat to the internet society, on the contrary, they provide a very valuable service to the internet as they help keeping systems one step ahead of malicious hackers or crackers as we discussed earlier [searchsecurity.com, 2001]

2.3.4. Black Hats

A black hat is a cracker that penetrates systems for his/her own benefit. He or she takes advantage of the revealed data by trading or by telling about the vulnerable system to others blackhats rather than telling the responsible organization itself. [searchsecurity.com, 2001]

2.3.5.Grey Hats

The gray hat is mix between black and white hats. He or she has no malicious intends but as grey hats find out about vulnerable systems the alert the involved organizations as well as the hackers society. This could cause other crackers to penetrate the system and sabotage it.[searchsecurity.com, 2001]

2.3.6.Script Kiddies

The script kiddies got their name from their reputation of gathering malicious software “scripts” and attacking networks with such scripts. They lack knowledge and they are destructive. As noted in whatis.com, hackers contempt script kiddies because they add nothing to the art of hacking, instead, they unleash the attacks of media on the hackers’ communities.

2.3.7.Lamers

According to the jargon file a lamer is an annoying beginner who is late behind in his cracked software, like in warez d00dz lamer, or in his knowledge like in crackers lamer. It also means that he scams codes of other crackers rather than understanding the concepts and making his own. [Raymond, 2000]

2.3.8.Cyber Warriors

“The final role that hackers may play, and the most disturbing, is that of “cyber warriors.” Yes, it sounds a bit like a video game. Unfortunately, in the not too distant future, and perhaps in the present, this may be more than science fiction. There have been too many rumors and news stories about governments building up teams of cyber warriors for this to be just fiction. Naturally, the press has locked onto this idea, because it doesn’t get any more enticing than this. Naturally, the public has no real details yet about what these special troops are.”

Nearly all types of infrastructure, power, water, money, everything, are being automated and made remotely manageable. This does tend to open up the possibilities for more remote damage to be done. One of the interesting questions surrounding this issue is how governments will build cyber warriors. Will they recruit from the hacker ranks, or will they develop their own from regular troops? Can individuals with special skills expect to be drafted during wartimes? Will hackers start to get military duty offered as a plea bargain? Also will the military be able to keep their secrets if their ranks

swell with the hackers who are used to free flow of information? [Rayan, 2000]

Actors in the cyberwarz are not limited to the previously mentioned. In fact there are many others which are distinct or overlapped with what was mentioned previously. Also, certain actors could claim to be of other category, for example, crackers calling themselves hackers. A very important note that must be mentioned in such content is that a person could experience many of these states as stages in his or her evolution to be a hacker. Elf Qrin [Cappello, 2000] discusses this issue more deeply clarifying the shifts between stages.

3. METHODOLOGIES

In this section we will exploit the three main levels for attacking a network. Each level contains different classes of attacks and information gathering techniques. The more an attacker sophisticates his or her attack level or methodology the more its likeliness to be a successful, clean and anonymous attack. The three methodologies are: a- simple attacks, b- professional hacking, c- strategic hacking. As we will see the attacks gets more sophisticated as we go on. And each more-sophisticated attack includes the techniques and methodologies of less-sophisticated ones.

3.1. Simple Attack

We will now describe the elements of simple attacks which is hardly could be called a methodology because it is so simple. However it is essential to understand it as independent technique due to its popularity. Script kiddies who are least sophisticated and most spread use simple techniques to crack into systems, as we discussed earlier these techniques are designed and coded by black or grey hats.

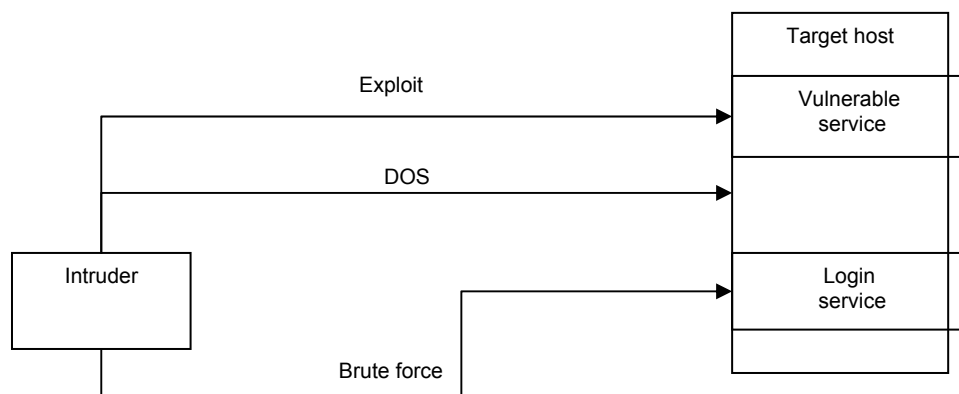


Figure 3.1.1 Simple Hacking

3.1.1.Simple Hack

A typical script kiddie will take a random alive IP address and start trying the scripts he has on. The scripts will mostly do one of two things:

- 1- Try to DOS this system.
- 2- Try to gain access to the system.

3.1.2.Gaining Access Through Exploiting a Vulnerable Service

Any given programs has bugs, these bugs could impose security breaches into that system. While some exploits are just sitting there waiting to be discovered, some other exploits needs a lot of hard work to make it work. Buffer overflow exploit are a good example of a well engineered exploit. In either ways script kiddies do not design or code the scripts or programs to do the payload, they just use it. Buffer overflow exploit depends on an idea called smashing the stack. When an arbitrary binary is receiving input it saves it in its buffer in the memory, the same old buffer that is keeping the return address for the program. Some function like “strcpy” just don’t check the input size and compare it with the buffer. This cause buffer overflow because the input string will overflow the return address for the function and the binary will crash. If the input to such function is well engineered it could replace the return address for the function and make it point to another privileged binary to be run for the intruder. This way an intruder could get access to the remote server. [Ryan, 2000]

3.1.3. Gaining Access Through Cracking Passwords

Another popular way to gain access to some service is by cracking its password. Password attacks could be performed on three levels, 1- simple password guessing, 2- dictionary attacks, 3- brute force.

There is no significant difference in the technique itself, the difference lies in the passwords that would be tried on the targeted host. An intruder could simply try some passwords that he thinks could be the one like trying the same user-name or user-name123. In the second technique he tries a file called the dictionary file. Some times this file could be of much less words and called word file. The script tries every word in the file as a password. Some advanced scripts add common strings like "123" to the strings in the file. The third technique is brute force in which the script runs all possible combinations of characters as the password string.

There are cases where password discovery process exists in some intersection between password cracking by try-and-error and exploiting a bug in implementation. Windows 98 share password implementation bug decreases the time needed to brute-force.

3.1.4. Denial of Service

Denial of service "DOS" is consider relatively easier to perform than other types of attacks. All the attacker does is stopping the service of some organization. This could be done by stopping/hanging the server that provides it, by stopping/hanging the service itself, or by cutting the road to this service by tampering with the network path to it. The most significant common properties of DOS are: 1- Its destructive nature. 2- Relatively easy, 3- Very high degree of being anonymous.

Denial of service may not be the most malicious act in many cases. The evaluation of how malicious an attack is depends on the targeted organization.

3.2. Professional Hacking

Hacking could be done in professional manner if the intruder followed a frame work that makes the attack much more effective. "Hacking exposed" illustrated the anatomy of a hack in way that helped us a lot in writing this paper. However due to the nature of our work we face situations that are slightly different from this anatomy. Next, we will describe the Hacking

exposed hack anatomy not typically as described in the book, but with the slightly different properties.

The anatomy of a hack consists of 10 process which are: a- Foot printing, b- scanning, c- enumeration, Gaining access, d- escalating privileges, e- Pilfering, f- covering tracks, g- creating backdoors [McClure, 1999] , and h- misinformation. [Ryan, 2000]

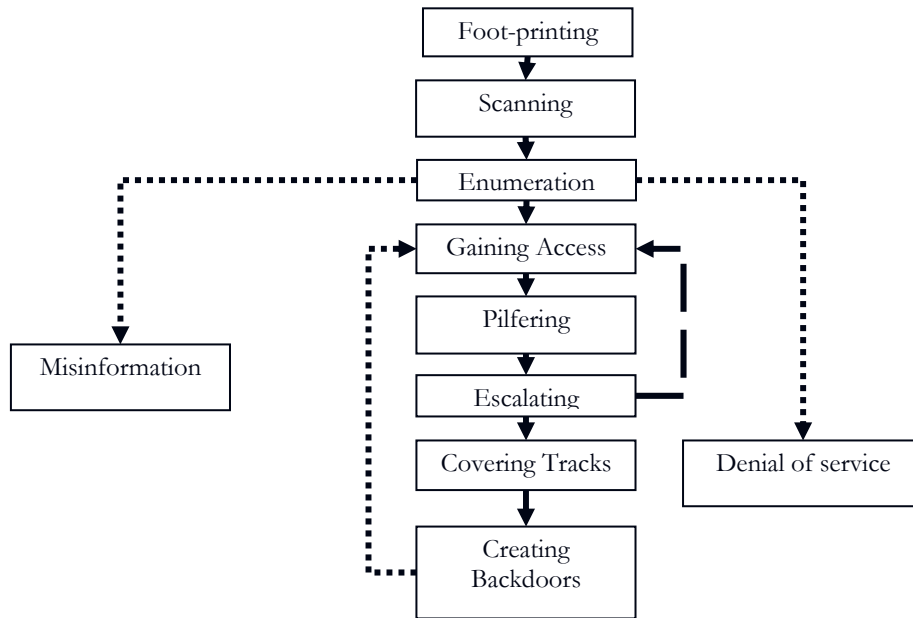


Figure 3.2.1. Professional Hacking.

3.2.1. Foot Printing

Foot printing is the initial wide-scale information gathering phase. In this phase the intruder gather all possible information about the targeted network. Gathered information include network addresses, manuals and attendance sheets and maybe even passwords from the company dumpster, hidden comments in the company’s website HTML source files, network routes to the company’s assets, stock and market details, merger and administration changes details.

3.2.2.Scanning

Step “b” the Scanning scans all the target networks’ resources in order to identify alive machines, their operating systems and the services running on these machines.

3.2.3.Enumeration

Enumeration tries to gather more information about every service. For example: the users and groups of the service, the version, and possible passwords.

3.2.4.Gaining Access

Gaining access is the phase where the intruder uses the knowledge gathered from the previous phases to get access to the system either by cracking a password or exploiting a vulnerable service. In this phase the intruder has an actual hand in the vulnerable system that enables him to start escalating his privileges.

3.2.5.Pilfering

Pilfering once again is an information gathering phase in which we want to penetrate trusted systems on the network. Now we could enumerate more systems and penetrate them.

3.2.6.Escalation

The Escalating privilege phase is concerned with upgrading user privileges to administrator privileges so that intruder has full power over the system.

3.2.7.Hiding Traces

Afterwards an intruder must cover his tracks, for example by deleting the logs and hiding his binaries.

3.2.8.Installing Backdoors

At last an intruder would install backdoors so he doesn’t go into the whole path again in order to own the system. [McClure, 1999]

3.2.9.Denial of Service

Two other phases are slightly different from the previous ones that are “denial of service” and “misinformation” attacks. The intruder could DOS

some services to serve a certain purpose in his attack scenario or just to stop the service if this is his only target. DOS is very helpful in accomplishing some targets, like for example: gaining access to Cisco router or disabling an intrusion detection system “IDS”.

3.2.10. Misinformation

Misinformation attacks like email relaying like DOS could be a target themselves but could also be a mean to social-engineer administrators or spoof orders to machines and destabilize operations.[Ryan,2000]

3.3. Strategic & Advanced Hacking

In the previous section we have seen how an intruder could plan to and attack a network. However, sometimes these steps are not enough to attack huge networks. If an intruder is after a huge secured banking network he should dedicate a great amount of time to plan the attack. The research has made some effort in merging professional hacking methodology with destabilizing networks methodology. The concept of destabilizing networks is based on extracting information about many aspects of the targeted network, then analyzing this information with many tools to determine the weak points in the network [Carley, 2001]. Figure 3.3.1 illustrates the merger between professional network hacking and network destabilizing techniques. The life cycle of the advanced or strategic hacking is hardly complete but it should give a clear overview of the whole process. The life cycle begins with a piece of information, for example, a trace, a company name, or an employee name. Even small amounts of information are very useful in footprinting a network. Unfortunately we will not be covering the details and steps of sub-phases like footprinting because they are out of the scope of this paper, we will only emphasize on destructive effect that a framework like –what we call- strategic hacking would have on organizations. The framework is divided into eight main phases which are: 1- Information Gathering, 2- Analysis, 3- Reliability checking, 4- Planning for the attack, 5- Initiating the attack, 6- Escalation loop, 7- Accomplishing the objectives, and 8- Ending the attack.

3.3.1. Information Gathering

The information gathering phase is very important. The accuracy of the analysis, planning and all the coming phases depend on the accuracy of this phase.

3.3.1.1. Foot Printing

As pointed before, we will not describe the detailed steps of Foot printing. However, an important point must be emphasized in this context. The open search as a step in Foot printing renders very important information. Imagine the intruder searching for the names and emails of the targeted organization's employees. Finding more details about them the intruder will attempt to attack their home computers as an easy totally unsecured privileged hop. For example, the employee may use the same password for the work and home computer, or he could be a workaholic who connects to a backdoor on his work machine to work late hours. Information like this could have negative impact on the organization's security.

3.3.1.2. Scanning

In a large network scanning could be a very tedious process especially if the intruder has to tweak his scanners to evade intrusion detection systems. This is another reason to emphasize the importance of a good Foot printing process that could lead to a more specific domain of machines to be scanned.

3.3.1.3. Enumeration

The information gathered in this sub-phase is very critical. The intruder tends to be very careful about the information gathered because this will be the essence of exploiting vulnerable services and gaining access to the targeted system. System administrators try to make this process harder by changing the banners and some messages in their system to delude intruders, but as usual there is more in identification than banners.

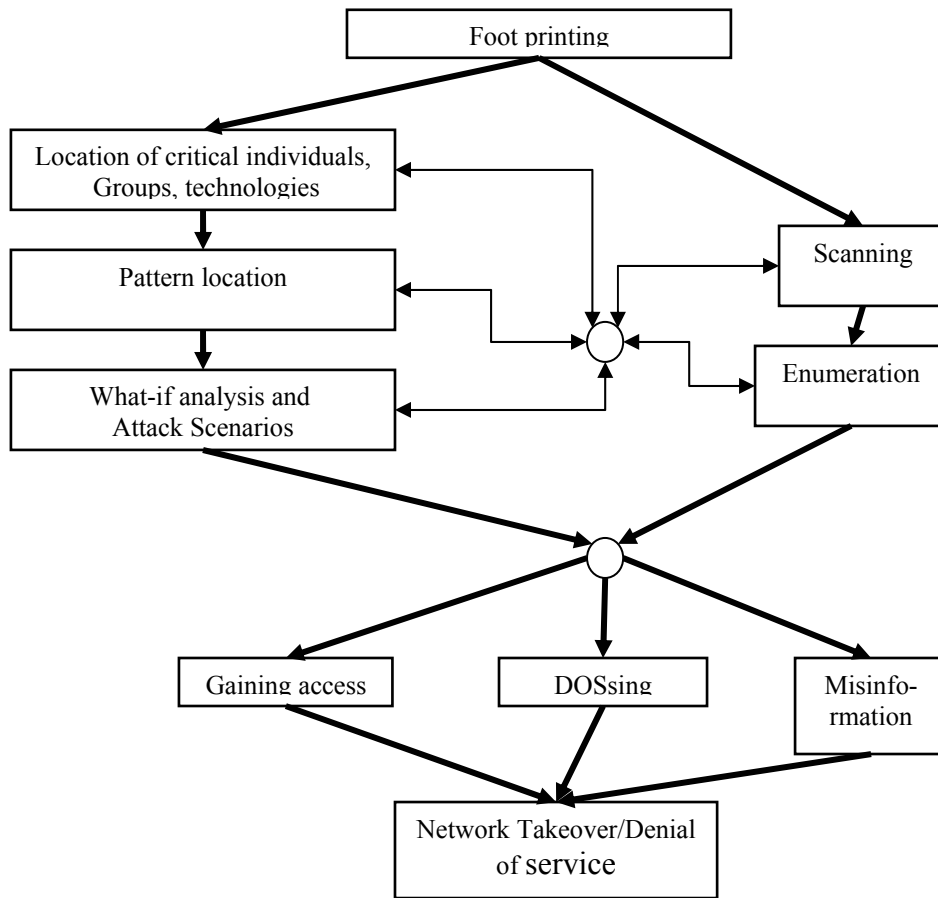


Figure 3.3.1. Simple Merger between Destabilizing Networks and Professional Hacking.

3.3.2. Analysis

The bigger the system is, the bigger are its bugs. Now that the intruder collected almost all possible data about the targeted network he begins the analysis. The analysis is dedicated to find out weaknesses in the network. The analysis is divided into three sub-phases: 1- location of critical individuals, groups and technologies, 2- pattern location, and 3- What-if analysis [Carley, 2001].

3.3.2.1. Location of Critical Individuals, Groups and Technologies

In this phase the intruder tries to locate entities and link them with their properties. For example, these groups could be identified in the targeted network: 1- Entities or groups that are if removed the network will pretty much affected, 2- Entities or groups that are unlikely to act towards different information, 3- Entities or groups that act fast to different information, and 4- Entities or groups that have relatively more power or authority. [Carley, 2001] There are many other entities that could be checked in Carley's paper for further details. Note that the research team is using the term "Entity" sometimes instead of the term "individual" to impose more generic concept.

3.3.2.2. Pattern Location

There are many pattern location techniques and tools that are very helpful in discovering patterns that are not visible to a man's eyes especially if combined with machine learning techniques. Some of the main points that should be identified in this analysis are: 1- the central tendency within the network, 2- basic components, 3- critical differences between sets of networks [Carley, 2001], as well as other points that should give the intruder a good idea about how to plan for the attack.

3.3.2.3. What-if Analysis and Attack Scenarios

The attacker begins to perform a what-if analysis based on the knowledge he has about the organization. "What if I target the mail server as the first hop into the network?", "What if I target the general manager computer at his home by hunting him down on an IRC channel?", and many other options. The attacker could end up with multiple attack scenarios ready for testing and initiation. As Carley [Carley, 2001] noted software agent models could render great results in such analysis, that is in out case, malicious results.

An important note is that there is a feedback relation between the information gathering phase and the analysis phase. Almost, always analyzing information raise new issues and uncompleted patterns that need more information to accomplish the analysis.

3.3.3. Reliability Checking

Now the intruder is ready to test his theory. This is important because if he is targeting a large network he is not performing a simple hack, instead he performs a sequence of misinformation, DOS, and gaining access attacks.

Sometimes these attacks will be scripted or automated. The intruder –as much as possible- will try to test these exploits. Two factors must be taken into consideration: 1- the timing of testing. 2- the efficiency of monitoring systems on the targeted test service, and 3- the behavior of those responsible of monitoring this service. On the other hand the administrator could be smart enough to recognize that something strange is going on, but could be busy enough to discard the whole thing!

3.3.3.1. Stealth-Testing the Vulnerabilities

This step is concerned with running the exploits on the well enumerated service, and making sure that when the time comes the exploit will work.

3.3.3.2. Brute Forcing Unmonitored Services

Sometimes, the intruder will need lots of time to brute force a login service. Brute forcing takes tremendous amount of time that's why it should be assigned enough time before the attack begins.

3.3.4.Planning for the Attack

Now that information gathering, analysis, and testing is done, the intruder has a good idea about what he will do and how to do it. He sits down to gather the toolkit and draw the attack trees, but certain critical issues must be put in mind while writing down his plan.

3.3.4.1. Sequence of Attack and Prerequisites

The attacker must organize his attack in way that clearly shows the prerequisites of each action. It will be even more professional to write down why these steps need each others as prerequisites. The more professional the attack plan is the more it's likely to succeed with little margin error. As pointed before, the larger the systems the larger are the bugs in it. This means that the huge attack scenario designed to attack the network has bugs that could turn a successful attack into an easy way to go to prison.

3.3.4.2. Semi-DOS, Flooding, and Reboot (Critical Timing)

An example of how timing could be critical is network devices. Some network devices when flooded or DOSsed fail opened. That is, to crash its access control system and keeping the accessibility for a certain amount of time. Even worse, some routers fall to its hardware authentication module with default password. In such cases the attacker must login to the router and

downloads the configuration file before the router restarts and gets back to its normal status.

3.3.4.3. Shifts and Using Exchange Times

Shift changing times are very useful moments to probe and start attacking the network. The first admin is getting too tired and bored to watch alert and the second is still sleepy because it's the 4:00AM shift and is trying to make coffee while listening –actually, not listening- to the first administrator telling him about the latest event or about something that he should checkout.

3.3.4.4. Attack Trees and Scenarios

At last the scenarios and attack trees find their way to documentation. The tool kit is prepared and scripts are containing all the ways that the intruders need to takeover the network. Embedding attack trees in scripts could make devastating result similar to what happened in the “nimda” worm. This work had four scenarios to gain access to a remote machine then using all these machines to attack the white house while turning the internet into a fragile worm nest by consuming its bandwidth.

3.3.5. Initiating the Attack

At the right time, the intruder begins the attack. Most of the attack techniques we discussed before, so we will be short and stress on some points.

3.3.5.1. DOS-Sing the Targets

Denial of service will be used to: 1- Disable monitoring systems. 2- Crash open access control systems. 3- Destabilize the network performance, and distract administrators and make them get busy with other things than monitoring the network.

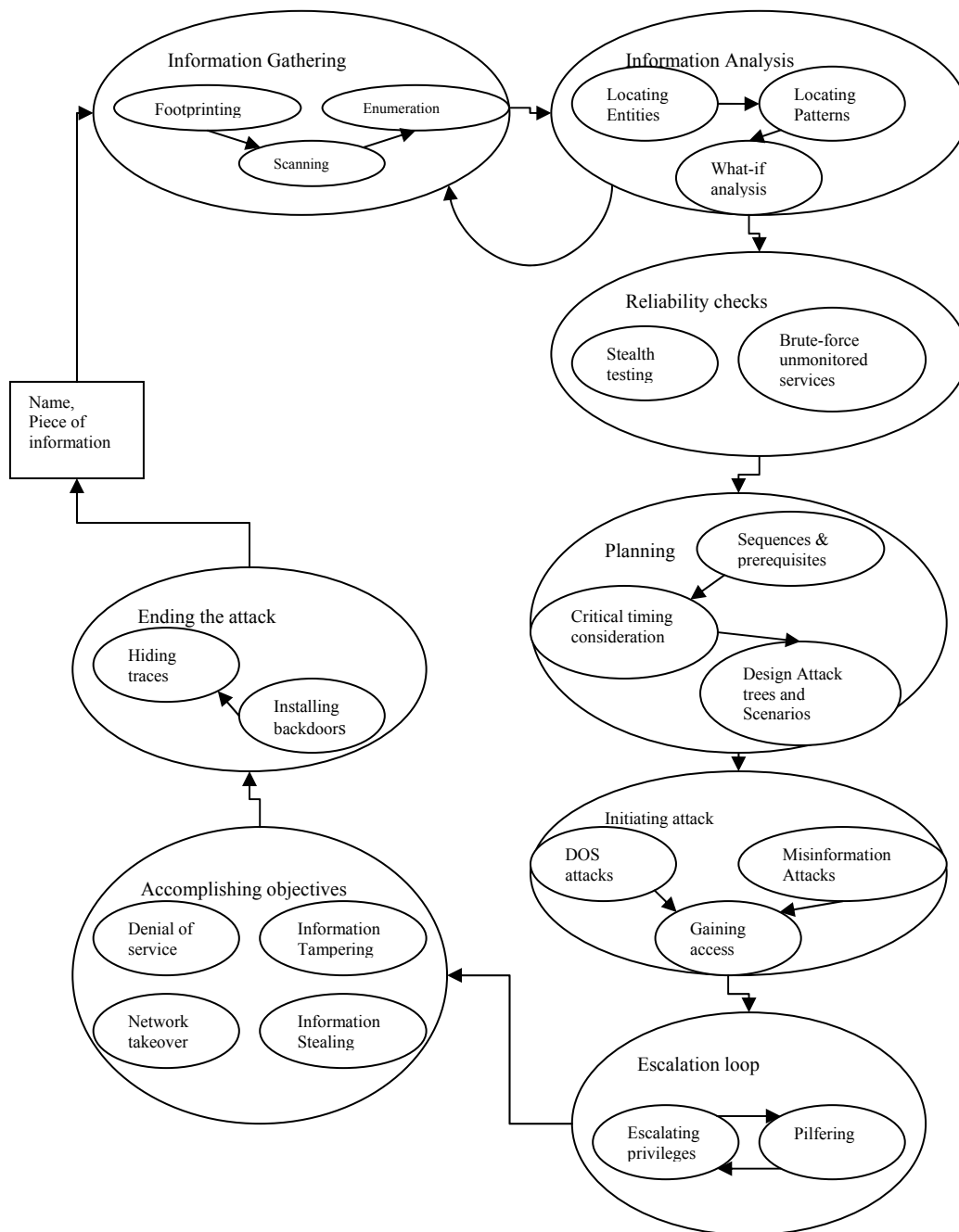


Figure 3.3.2: Advanced hacking life-cycle

3.3.5.2. Misinformation Attacks

Combined with DOS attacks misinformation attacks could be very powerful in: 1- distracting administrators. 2- Making it very hard to trace the real attacker network address. 3-making Denial of service un-block able by changing the packets' source addresses rapidly.

3.3.5.3. Gaining Access

When the attacker finally receives a success acknowledgement from a vulnerable server through a cracked password or an exploitable service he know that he has little time to escalate his privileges to gain full control of the compromised server. The escalation loop begins.

3.3.6.Escalation Loop

This loop could iterate many times till the intruder gains full control of the targeted system. This system could mean a server or the whole network.

3.3.6.1. Pilfering

The intruder pilfers more system information that will be –most of the time- easier to get now that he has a hand in the network. He looks for trust relationships, passwords by sniffing, and more.

3.3.6.2. Escalation

Now the intruder uses this pilfered information to escalate his privileges. And the loop goes on till he accomplishes his objective which could vary from an attacker to another according to their motives.

3.3.7.Accomplishing the Objectives

The main technical objectives we may think of are: 1- Taking over a system, 2- Deny a systems service, 3- Stealing critical information, and 4- Tampering with critical information. They may not be all technical objectives for an intruder but they are sufficient for the needs of this paper.

An attacker could have more than one objective to accomplish. For example if he wants to ruin a companies reputation, he could deface its website (data tampering), shuts down its mail server preventing it from communicating with customers and suppliers (denial of service), and downloads its clients database to be distributed (stealing critical information). Accomplishing all theses technical objectives will accomplish his main goal “ruining the company reputation”. Also if the intruder managed to take over

the network or at least a great deal of it he'll be able to pay it some really disturbing visits later on.

The intruder may also accomplish objectives other than his main to make it seem like he is doing something else to elude the forensics people so he would be more anonymous and/or be able to come back in a less dangerous environment.

3.3.8.Ending the Attack

Now the intruder begins the last step. There are two objectives for him now: 1- keeping himself anonymous, and 2- providing a way that enables him to come back for some malicious actions later on.

3.3.8.1. Installing Backdoors

Backdoors vary in nature, they could be normal services secretly running on a different port, or they could be special binaries made specifically for this purpose. It is important that these backdoors be hidden from the eyes of the administrators.

3.3.8.2. Hiding Traces

The very last step to finish the job is hiding the traces. Clearing logs, removing intermediate accounts, and deleting or hiding the malicious binaries used to compromise the systems. The attacker logs of the network and the internet after this long sophisticated job.

4. SCENARIOS AND CONCLUSIONS

In this section two common scenarios will be presented to show how strategic hacking could be used to electronically terrorize important governmental and commercial entities over the internet. The first scenario is concerned with terrorizing governmental agency on the internet by taking over its network. The second scenario will attack the business of a commercial company by a simple but effective attack that is denial of service.

4.1. Takeover Scenario

4.1.1. Actors, Motives and Assumed Structure

The targeted network: A governmental unit that provides computerized license renovation.

The online service is not yet running but is being developed.

The time: Nothing specific.

Intruders: Someone who has interest in making the electronic government project fail. So, he hired a professional team of intruders (hackers/crackers) to do the job for him.

Motive: He wants to take over the network so he could manipulate it anytime he wants to prove something. And if have to he would want to destroy all the data in the network.

Figure 5 illustrates the details of the Targeted Network.

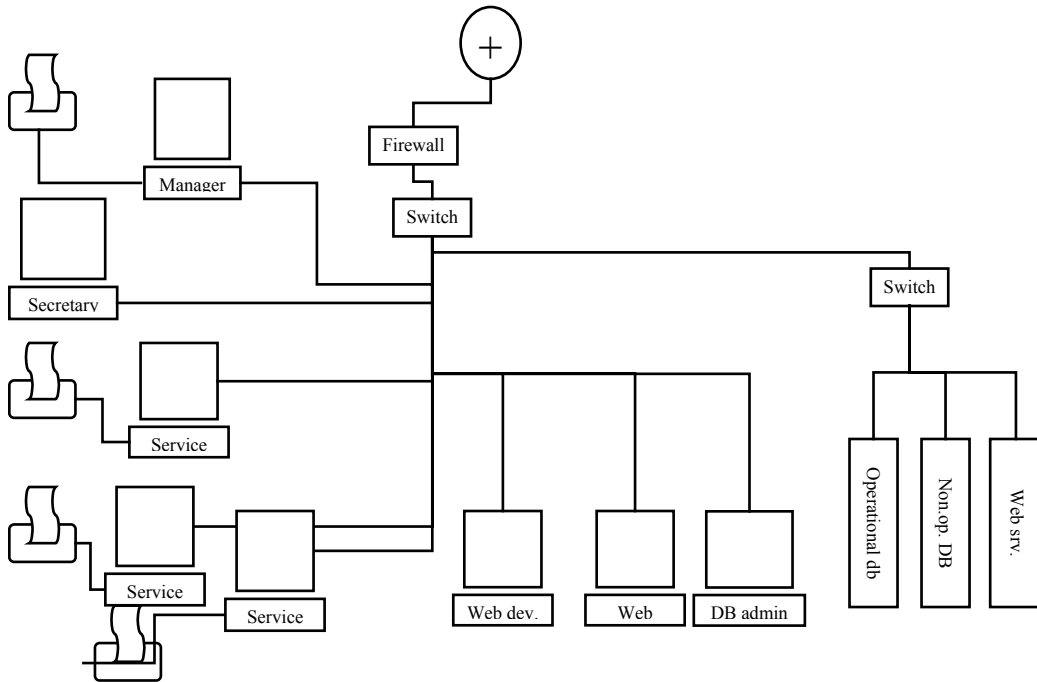


Figure 4.4.1. Targeted Network

4.1.2. Attack Scenario

The number of different combinations of attack scenarios is too large to be counted in this paper, but we will try to show in every step a sample of what could happen.

4.1.2.1. Information Gathering

4.1.2.1.1. Foot Printing

The Intruders team begins to gather all possible information about the unit. The team comes with the following results:

- 1- The secretary e-mail from the website.
- 2- The IP addresses for the network xxx.xxx.xxx.0-31. All real IP's.
- 3- A good idea about how the system works by going to the physical place and asking how to renovate a license.
- 4- The intruder notices that there is a room called "the server room".
- 5- The developer is a graduate of a different OS platform than administrators. This could mean non-standard Operating systems.

4.1.2.1.2. Scanning

The team starts stealth-scanning the range and gets the following results:

- 1- The firewall is badly configured to block only suspicious ports. It should have been a "deny all allow only what you need" policy.
- 2- The attackers presume that the firewall also allows all outgoing traffic.
- 3- The Machines scanning results are as following:
 - a. Web server is listening on: 1- 80, static pages. 2- 8080, some dynamic pages the developer is developing for the forthcoming service.
 - b. Operational database server: apparently the SQL server port is filtered as it shows from the scan.
 - c. Non-operational DB server: SQL port is opened as well as terminal server port.

4.1.2.1.3. Enumeration

Enumeration results:

- 1- Web server and operational database servers are updated with patches and have antivirus.
- 2- Non-operational database server is not.
- 3- Manager machine is sharing the printer and a writable folder.
- 4- All service machines have the names service-3 and username and password service.
- 5- All client machines are windows 2000.

4.1.2.2. Analysis

4.1.2.2.1. Location of Critical Individuals, Groups and Technologies

- 1- The secretary machine usually is less secured but has more information about the company than the whole company.
- 2- Web developer machine usually has more privileges than normal users but the developer most of time is not keen on security as administrator.
- 3- The technical group (web admin, database admin and developer) has access on the servers group.
- 4- The server group is in a separate room (maybe on a separate hub).
- 5- Only two users on the administrators' machines. This implies that the two different administrators (DB, web) most probably know the system's, web's, and database's password to be able to fill in for each others.

4.1.2.2.2. Pattern Location

- 1- The service machine is a pattern.
- 2- Having terminal service on the non-operational database could be a pattern on other servers.
- 3- The password for the servers could be similar (a pattern). If we could sniff one, we would get the rest.

4.1.2.2.3. What-if Analysis and Attack Scenarios

The intruders have a couple of options as an entrance point:

- 1- Send the secretary a Trojan horse.
 - a. They could find critical information about the manager, the company, and maybe even backup of the source codes and databases.
 - b. They could find old password or any other critical in mail boxes.
- 2- Attack the un-armored web server on the developer machine.
 - a. They will be able to get the source code and designs.
 - b. This goes for all client machines: they will sure gather new information and use it to sniff at least local password, brute force other machines, and make misinformation and DOS attacks.
- 3- Attack the SQL server on the non-operational server.

- a. They maybe able to sniff passwords of the hub.
- b. Download the data of the server.
- c. Know the structure of the operational database and try to send queries.

4.1.2.3. Reliability Checking

4.1.2.3.1. Stealth-Testing the Vulnerabilities

The team tried a couple of exploits and they worked.

4.1.2.3.2. Brute Forcing Unmonitored Services

The intruders were not able to brute force NetBios services due to the firewall so they postponed it until they have a hand on the network.

4.1.2.4. Planning for the Attack

4.1.2.4.1. Sequence of Attack and Prerequisites

The intruders' team decided to attack the network with the three options they have. The attack will take place after the units working hours. They made sure the secretary got her fancy screen saver Trojan in the afternoon when she is too tired to work or think.

4.1.2.4.2. Attack Trees and Scenarios

The attack tree is drawn every intruder knows his part. The tool kit is ready.

4.1.2.5. Initiating the Attack

4.1.2.5.1. Gaining Access

Administrators are not available so there is no real need for misinformation attacks. And there are no IDS to DOS. They gain access nice and easy.

4.1.2.6. Escalation Loop

4.1.2.6.1. Pilfering

The intruders install their sniffers. They brute-force "netbios" from within the network. They gather and download every bit of

information they are able to get. They also find out that web server and operational database server have terminal service on.

4.1.2.6.2. Escalation

They get access to the service clients. They get access to operational SQL server the famous exploit of the SQL worm, and so on.

4.1.2.7. Accomplishing the Objectives

After three or more escalation loops in about a week the intruders group have almost all the passwords of the network. They are ready to do whatever their employer asks them to do.

4.1.2.8. Ending the Attack

4.1.2.8.1. Installing Backdoors

The intruders install 2 instances of “netcat” on the server. The first one will act as a server. The other one will act as a client that tries to connect every week to a previously compromised server by the intrusion team.

4.1.2.8.2. Hiding Traces

The team executes a root-kit that erases the logs, hide the binaries and erase any users they may have added to some systems.

4.1.3. Impact on the Organization

Invading the privacy of at least thousands of citizens which could very much compromise the electronic government project in Egypt.

4.2. Denial of Service Scenario

4.2.1. Actors, Motives, and Assumed Structure

The targeted network: A company that makes online reservations for vacations.

The time: right before summer vacations begin.

Intruders: the web admin of a competitor website.

Motive: the intruder website is not making enough profit, so he decides to stop the better competitor’s service to direct the customers to his website.

Figure 6 illustrates the details of the Targeted Network.

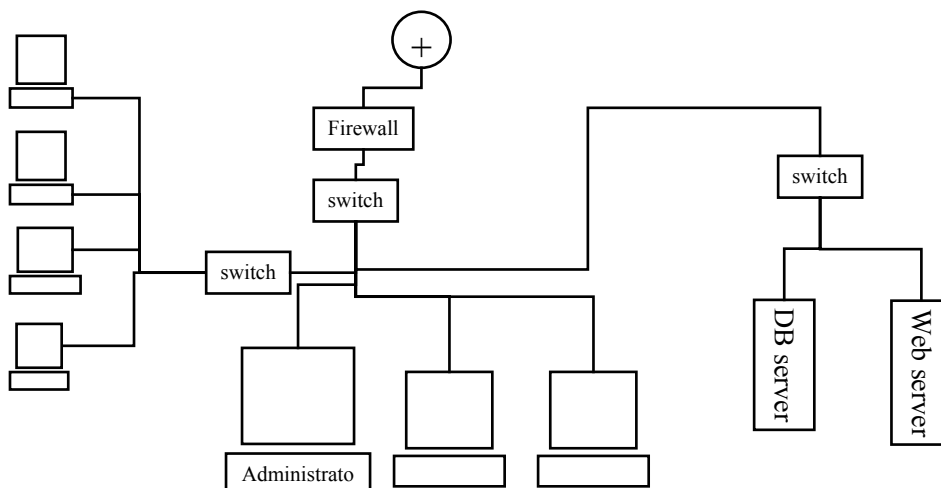


Figure 4.2.1. Targeted Network.

4.2.2. Attack Scenario

The scenario is not a complicated one although it's a very destructive and it costs the targeted organization a lot of money, time, and effort.

4.2.2.1. Information Gathering

4.2.1.1.1. Foot Printing

The Intruder begins to gather all possible information about the unit. He got the following results:

1. The IP of the website.
2. The IP addresses for the network xxx.xxx.xxx.0-12. All real IP's.

4.2.1.1.2. Scanning

The Intruder starts stealth-scanning the range and gets the following results:

1. The firewall is badly configured to block only suspicious ports. It should have been a "deny all allow only what you need" policy.
2. The Machines scanning results are as following:
 - a. Web server is listening on the following ports: 7 echo, 19 chargen, and 80 http.
 - b. Operational database server: apparently the SQL server port is filtered as it shows from the scan.

4.2.1.1.3. Enumeration

Enumeration results:

1. Web server and operational database servers are updated with patches and have antivirus.
2. The router is vulnerable to “EIGRP DOS” Attack.

4.2.2.2. Analysis

The scenario doesn’t require analysis as it’s purpose is only a destructive and it’s easy to be done.

4.2.2.3. Planning For the Attack

The intruder has two ways to attack the network:

- 1- Initiate DOS attack on the router.
- 2- Use the “echo-charge” vulnerability to DOS the web server.

The intruder chooses to use only one attack per time just to make the administrator confused.

4.2.2.4. Initiating the Attack

The intruder starts the attack by:

- 1- send a forget packet to the web server “charge” service that pretends it came from the web server “echo” service. This will cause a loop between the two services consuming the full processing resources.
- 2- Send forget “EIGRP” packets to use the “EIGRP DOS” router vulnerability.

4.2.2.5. Escalation Loop

There is no escalation loop. However, the intruder will repeat the attack scenario whenever the need arises.

4.2.2.6. Accomplishing the Objectives

The objective of the mission which is denial the online service of this company is accomplished.

4.2.3. Impact on the Organization

Let's assume that the company makes on average 100\$ per hour, the intruder manages to DOS it for at least 16 hour/day. So it will cost the company about 1600 \$ per day.

4.3. Conclusions

Malicious hacking or cracking is not a harmless hobby, in fact it, malicious internet intrusions cause companies great deals of money, effort, and time. Malicious hacking could be motivated by many motives; one of them is electronic terrorism. Advanced or strategic hacking is could be used to terrorize commercial as well as governmental organizations by stopping them from providing their services. However, keeping the organization from providing its services may not be the greatest threats it faces on the internet. A well design attack may compromise the organization's integrity. Such attacks could also threaten national projects like electronic government. Facing such threats is a must.

5. COUNTERMEASURES AND RECOMMENDATIONS

This small section will list some of the different groups pf countermeasures and make recommendations based upon the conclusions of this paper. However, there are a variety of countermeasures which is also out of the scope of this paper. So, we will only emphasis important point regarding countermeasures.

5.1. Countermeasures

We could divide countermeasures techniques into two main groups for simplicity, 1- Basic, and 2- intelligent. The basic grouped contains techniques for armoring the systems, building access controls, backup, logging, fall recovery, and intrusion detection. The intelligent grouped contains techniques for: making honey pots, intelligent intrusion detection systems, and forensic analysis.

Two important issues in designing a good security solution are: 1- Good policy and procedures, and 2- integration. We cannot give a good policy/procedure designing too much credit. Whatever security tools are installed and operated, these tools could be a waste of time if there is not well designed policy and procedures behind their installation. The other important

note is the integration between these security tools to perform more efficient security system and more reliable detection.

5.2. Recommendations

The cyberspace is a new world with lots of potential and opportunities. To be pioneers in this world or at least to have our share of it we should know. Egypt must invest in the human to be specialized in the cyberspace internals. Hacking as pointed out in the first section is about understanding this cyberspace. And, for any organization, in order to able to secure itself it must invest in internet underground knowledge. Unfortunately this is very expensive even for big organizations. The recommendations of this paper is easy to write yet hard to accomplish. And they are:

- 1- Developing a research and development institution for cyber security that should provide solutions and consultation services for the governmental as well as the private organizations.
- 2- Increasing the awareness of people in the field of cyber security to increase the possibility of a new generation that could explore and develop this new space.

5. REFERENCES

[Cappello, 2000] Cappello(2000), HACKER STAGES v1.0., www.elfqrin.com/docs/HackerStages.html.

[Carley, 2001] K. M. Carley, Ju-Sung Lee and David Krackhardt (2001), Destabilizing Networks, *Connections* 24(3):31-34.

[Fisher, 2002] Fisher, V.(2001), E-Terrorism: An online war?, <http://news.zdnet.co.uk/story/0,,t269-s2126759,00.html>.

[McClure, 2001] McClure s, Scambray j. (1999), Hacking exposed, Osborne / McGraw-Hill.

[Nolan, 1996] Nolan, J.(1996), What is Competitive Intelligence and What Can It Do To Us, <http://www.intellpros.com/lib/what.html>.

[Raymond, 2000] Raymond, E.(2000), The jargon lexicon, www.catb.org/~esr/jargon/html/H/hacker.html.

[Ryan, 2000] Ryan R.I, Stace C., Mudge (2000), Hack proofing your network, Syngress, Media.

[searchsecurity.com, 2001] www.searchsecurity.com.

[Thomas, 2001] Thomas, B.(2001), U.S. to Intensify Effort against Threat of Computer Terrorism, www.latimes.com/news/nationworld/nation/la-100901cyber.story.

[whatis.com] www.whatis.com

[Winkler, 2001] Winkler, I.(2001), Are companies really ready for e-terrorism?, www.zdnet.com.au/newstech/security/story/0,2000048600,20261574,00.htm