

Breaking the Perimeter Through the Human Stupidity

Oliveira, Bruno Gonçalves. bruno@bsdmail.com
Londrina - Parana - Brazil

Abstract

Software vulnerabilities nowadays (there's a time ago) are not the main factors for possible attacks in a corporate system. The attacks based on social engineer and no tech hacking are increasing more and more. This all happens because the weakest point continues being the human. Every failure created is always by man, so if we take advantage not just in a computer way, but a way for the computer, we can get many things more, this paper tries to make an overview the logical ways for bypassing security infrastructure and do a comparison with some techs created for testing security structures utilizing the people inside and trust in a dummy configuration. This research was based on my environment life, so the opinions around the world can be different.

1. INTRODUCTION

In a penetration test the first thing tried to compromise the target, is the perimeter, if it's easy, the exploitation will be easier too, a lot of researches developed techniques for bypassing firewalls, IDS/IPSs, etc. And, as expected, the security companies work hard for trying to decrease the risk and getting better, but what happen if the administrators don't follow the vendor and don't study new stuffs? The technology just being not used or bad used, just wasting money.

Observing the tendencies of penetration tests in the past years, we can see an evolution, mainly when we talk about big companies that has improved security features, no problems with updates, etc. In this case what almost happens it's used the client-side attack, and this comes together the social engineer for gathering information, and that can be a valious tip for the perimeter as well and studying my local environment it's notable that the administrators doesn't know or even care about some stuffs.

Good technologies are being created and developed for the perimeter like NAP (Network Acces Protection) from Microsoft and NAC (Network Admission Control) form CISCO, those ones are a greate defense, if were well configured and that's the problem, they have a lot in their hands and don't know how to act.

Despites of a lot of tools that we have for this, but we have so many impracticables for misc reasons not treated here, but it's easier and more fun when we can play wth people. Before these techniques explanations, it will be compared with the well-known ways to do that, technology.

This paper will debate about bad configurations in structure and use of social engineer for geting information in a real world.

1.1 Motivations

The main purpose of this work is evaluate the administrator's knowledge and the users' culture, as part of my job, perimeter is essential and has to be extremely well carefull. Failures on firewalls, for example, can facilitate a lot the attacker's life, and when I apply failures, is not software vulnerability, but when the admin write the rules for lazy or another thing, they believe in miracles and don't believe that the worst can happen with them.

2. OLD SCHOOL TECHNIQUES

In this chapter, it will be approached the old fashion techniques used for bypassing the perimeter protectors, Firewalls and IDSs, commonly used. Perimeter doesn't have many security resources, but some companies are trying to defend more utilizing new technologies that can be a great help.

The intention for putting this techniques in the paper is just for knowledge and expose technology failure as well before the human mistakes.

2.1 Firewalls

The first thing thought when talked about perimeter, is the firewall, the main and more adopted security feature in the world. The firewall is just based on protocols and controls the traffic between 2 or more points, allowing or dropping packets from the sources, observing that we can try a lot of flags' combinations in packet for try it.

2.1.1 Traceroute and TTLs

The primary way to do the test with the firewall, and well known, it's the use of the next hop of the firewall, with that hop in hands we can determine the next routers in the network and discover what ports are opened for traffic.

The IP TTL, that's a field used to limit the lifetime of datagram, is decreased when a router forwards a packet, and if TTL start at one, we can find routers in a traffic just increasing it. With this information in hands we can set the TTL that you want and your ACL filter TTL and with tries and errors guessing what port is opened for traffic.

The softwares traceroute and firewalk are good choices for that. Too explored so it's not necessary explain how to use.

These are old techniques and maybe in a statefull configured firewall not allow, because, even the request is in UDP, the response for time exceed and dropped packet is in ICMP and it's necessary to be allowed this traffic for working.

2.1.2 Tunneling

Knowing what ports are opened for traffic, the things get better, we can enjoy this opened door creating some tunnel for communication with others protocols.

It's through like a VPN, all traffic in one protocol with encryption, a lot of softwares can be used for that.

2.2 IDS

IDS are largely implemented for attacks detection, there are many IDS on market, so vulnerabilities depends on what you are implementing. Therefore, this paper won't talk about a vendor, but in the most cases the Intrusion Detection Systems are based on signatures, and that's what will be exploited, in next sessions we will review some techs for bypassing signatures.

2.2.1 Payload Change

It will be showed some techniques, those were used for bypassing IDS/IPSs Systems, in some cases vendors can be patched, this is a simple list of some vulnerabilities found in IDSs.

There are a lot of techniques for this intention, and new ones are being developed every day, those ones were just for illustrate. We have to be in mind that what we need for bypassing is change the most used for another thing different.

- URL Encoding

RFC 1738 states that only alphanumeric and special characters can be included in the URL and this encode allow those ones to be passed to the web server via the URL.

-Canonicalization

Canonicalization is put something in a simplest form, it's a good practice put everything you wanna do in this way, maybe can bypass the system.

-Unicode

Any character is represented by two octets: "\" is encoded as %c1%9c for example, so if the IDS are not ready for receiving that request, it will accepted and not alerted.

-Null bytes

In some cases, if you put a %00 in the final of attack you can change the signature and bypass IDS as well.

-Sensitive Case

cmd.exe is different of CmD.eXe, so sometimes work.

-Transform binary in hexa

Another point interesting for changing you payload that's in binary in hexa.

2.2.2 Splitting the traffic

Another way for bypassing IDSs is fragment the traffic, if you transmit in separates packets like GET in 3 packets not just in one, the IDS doesn't understand the traffic and allow without alerts. Tools are developed for that purpose, a great one is the tcpreplay, see in the references.

2.2.3 Create a crypto tunnel

IDSs don't work on cryptografed packets, obviously, because it doesn't understand what is passing through it, so creating a tunnel for transmit crypto packets can bypass the protection.

3. BREAKING IT WITH PEOPLE

Now, we begin with the real goal, that's expose some techniques tried and with no knowledge of the environment begin a sucessfully attack on host. This is a real test done in some companies, allowed, that we can observe why people suck, the same technique on everyone.

Studying, it's not hard to see that the social engineer tech is enjoyed by many pen-testers, but in the most of time it's used for getting stuffs that's even the non-trained people knows that is confidential, we know that despites of they know, they pass, but let's try to be less notable.

Taking a look in the target, just by the name, we already know that it's a big company and must implemented a lot of security features,, not just automated tools will solve our problem, how is implemented them is our chance.

As said before, not just the social engineer will be used but some infrastructure common errors that enables a full access in the entire organization too.

This study is not just related to blackhat test but a gray test as well, a company that don't worry about disgruntled employees, don't need to worry about external too.

3.1 Technology underused

The existing technology in the environment doesn't prove if the company has an good security, in the most of time the feature implemented has much more to offer then actually is used, this happens because the people are not ready and even an expert has deployed, the maintenance and the updates are not done.

One of the most used feature in security, is also the worst implemented, the firewall, the concept for preventing arbitrary and unnecessary traffic is lost, at least in the most companies that were researched.

In rules case when admins are testing some new service or disable something some rules are created, but even when is disabling or enabling the new things they didn't erase them, so you have a lot of rules that allow traffic that is unused but can be for compromising the target.

It's doubtful that when you are looking at a firewall rules you didn't see anything that wasn't to be there, rules contrarying others, sometimes it's not in the script, but when you list the rules, some rules applied that nobody knows why they're there.

Another one, it sounds funny, but common, it's full access from INTERNAL > DMZ, and from DMZ > INTERNAL. The DMZ is implemented for preventing the attacker to see internal stuffs and even with this thinking, the rules are full and serious problem is done.

A big mistake done by many administrators, is WHERE put the firewall, and what it will cover and depending on where you are implementing you have to see around and select the best one.

A good practice is that all routers and networks must be plugged in a firewall because if it's not, it's possible to take another route. A fool example it's if you plug the modem cable into a same switch that is the lan or a protected network like DMZ, you can bypass all traffic to those destinies.

Another system too mistified by the administrators, deployed and managed with errors it's the IDS what with no knowledge let it with no benefits for the environment.

Researching these feature in a lot of places, it's not hard observe how is implemented, in the most of case in auto-pilot (thanks Sp0oker), everything is done by default instalation without different rules.

If the analyst doesn't know how to write rules for the IDS, he doesn't know how to interpreter, so the use is just being unnecessary.

Sometimes the administrator buy the solution thinking that's the salvation for the network, and even know how it works.

So, if you catch the rules implementes (vendors site) and you wanna explore one of them, for sure, you can find a way, when we already have the pattern and they didn't modify anything, ready, a few characters more or less and it's done, bypassed.

3.2 Technology not used

Researching about structure, it's common find some erros like the administrators that don't understand the power of users and expose all local servers and don't separate them from the local network, in researched places 100% happens that, the maximum done is separate in VLANs for management.

When is implemented the DMZ, the purpose is preventing possible attacks to walk inside the local network and local servers, so seeing the attack number currently it's clear that the dangerous intruder now is the employer, so the insouciance in relation with that can compromise the company at all.

It's not new that disgruntled employers (actuals too) can do a serious damage in a structure and cause financial injuries, reports based in this type of attack present that.

About logs, some administrators even see what happens in systems or security structure, the arrogance doesn't let the people related to iT get more envolved with that, the trust beetwen what is already implemented and the administrators confuses at all, logs are really interesting and can demonstrate with details how is the structure implemented.

3.3 Social Engineer

A great opportunity for testing employers and co-related in your environment is doing a social engineer attack, like demonstrated in the demo, we can easily catch many resources about the company including its perimeter information with it.

Currently very utilized in penetration tests, the technique involves personification and tries collect good stuffs from the company.

There are many kind of this attack, if you can persuade someone for giving information, you are doing a social engineer attack. For the targets, a lot of information are not confidential because they don't know what is and explore that turn the attack more interesting.

The social engineer attack trust in innocence and the pentester must bring comfort to the targets, with a good chat what you need know you will. I think that the great point is the ignorance, the targets don't know what can or cannot compromise something.

Doing tests with the people, it's possible with some common tools demonstrate how fragile is the perimeter and find out which way we will attack the target attaching others attack for exploiting it.

4. DEMO

In our demo, I will show how information gave by a non-tech people inside the corporation that can collaborate for bypassing the perimeter from external location. This test was allowed by the company.

In next steps, some information will be covered for obvious reason, we are in real world.

- First Step: Gather information passively

Gather information about the company, easily in a short research it was determined the domain, until that we just had the name, as a big company Google finds fast.

Consulting the routers I can find the who is the ISP and that information can be used for inducing the victim.

With the domain, we can take, in the most of time, the responsible of IT department, with you are not sure, try something else, like below, and in the site we have the phones, for a while that's all that I need.

-Second Step: Gather information about perimeter (social engineer attack)

In the recorded chat in a phone call, I pretended to be a employer of its ISP, talking about internet problems and asks for some tests, for proving that I know the environment, in the first call I persuade the person for telling me the name of IT guy, and with that information, it's easier get involve with the next

5. CONCLUSION

In a real world, sometimes, things that we feel possible to do we do not, this happens because the security preoccupation increased and simple attacks are not effective even bad configured the improvements, it does a nice job but the people conscience still doesn't change, despites of a lot of technologies are being released for support the IT department, the related employers don't care too much and the lack of experience turns the environment still too much vulnerable.

It's not so simple do this job and if the pen-tester is not used to make it the target will mistrust and attack can fail easily but if he was well successfully, he can demonstrate many vulnerabilities in physical access and in the human credibility.