

CFP

Author: Bruno Goncalves de Oliveira, bruno@bsdmail.com, +55 43 99726819

Hacking from the Restroom

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.

Detailed Outline:

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/IPSSs, 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.

Bio:

Bruno Gonçalves de Oliveira, computer engineer, security analyst at Altatech -Londrina/Parana/Brazil, holds some certifications, develops techniques to attack systems for profit == fun, does security structure analysis, applies defense tactics with softwares, hardwares and trainings. applies pentest for investment directions on info security and to assessment in a real world of actives in iT environment. And still researches about network security for acting in his current work/job, these works became talks at security cons like H2HC IV, YSTS 2.0, ToorCon X and already accepted for YSTS 3.0