iBLISS

Bruno Gonçalves de Oliveira
bruno.mphx2 *nospam* gmail .com

breaking the perimeter through the human stupidity

$whoami

- Intrusion Analyst at iBLISS
- Computer Engineer
- Holds some certs
- Over 9 years studying/working/having fun with security;
- Spoken at HITB Malaysia 2009, YSTS 3.0, YSTS 2.0, Toorcon X (EUA) and H2HC IV;

iBLISS

Agenda

- The Beginning
- Motivations
- Perimeter Security Technologies
- Breaking the perimeter with…
  - NOT USED
  - UNDER USED
  - SOCIAL ENGINEER
  - Samples
- TOOLS
- DEMO
- Conclusion

iBLISS

The Beginning

- Most of time, first thing to do!
- Security features created day after day.
- Client-Side is being the choice by many pentesters;

iBLISS

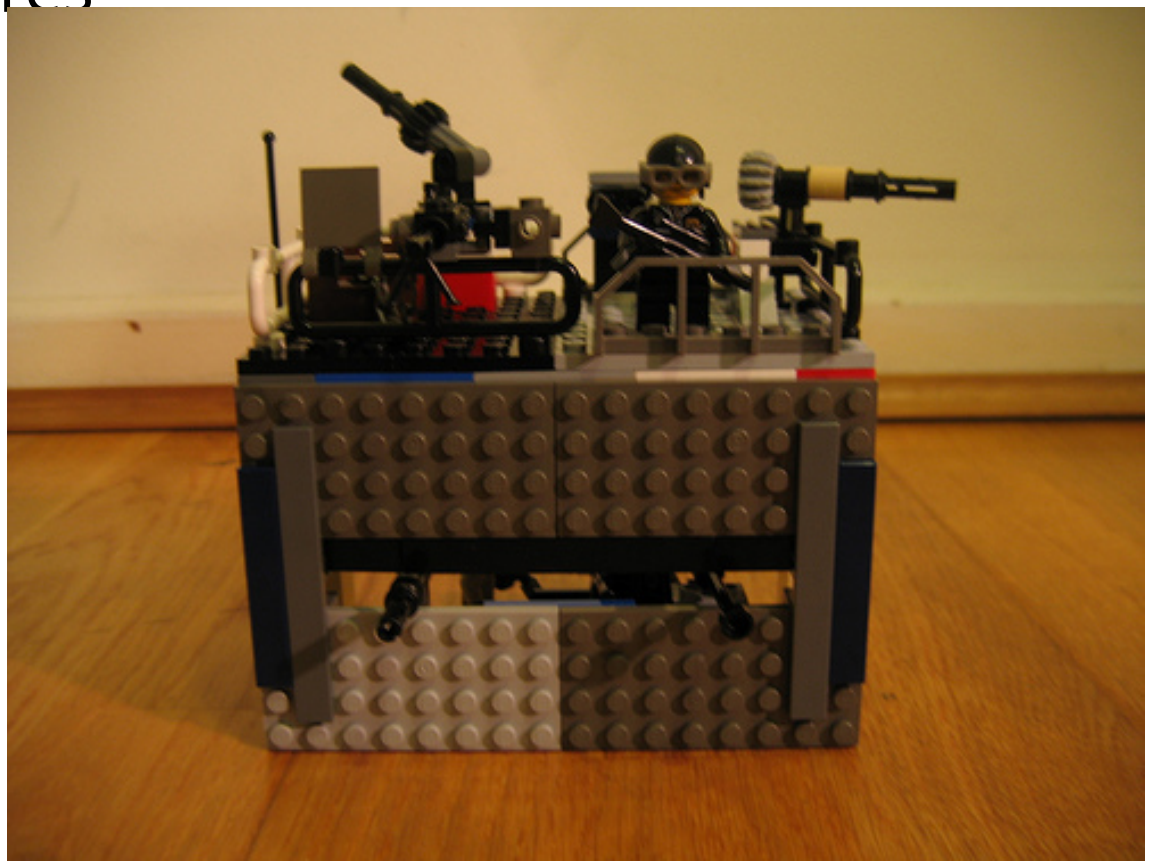
Motivations

- People are always fun! ;)
- Improve admins' knowledge.
- Evaluate users' culture.

iBLISS

Perimeter Security Technologies

- Network Structures
  - Routers
  - Switches
  - Design
- NACs
- Firewalls
- IDS/IPS
- AVs



iBLISS

breaking the perimeter with…

- Technology NOT used
- Technology UNDER used
- Social Engineer

iBLISS

NOT used

- Structures available and nobody to configure;
- People doesn't know the power that they have inside;
- Same money but more effective;

iBLISS

Samples

- LOGs > It's rare see people that REALLY analyse LOGs file.
- Switches/FW/Routers > Why your network is a mess ?

iBLISS

UNDER used

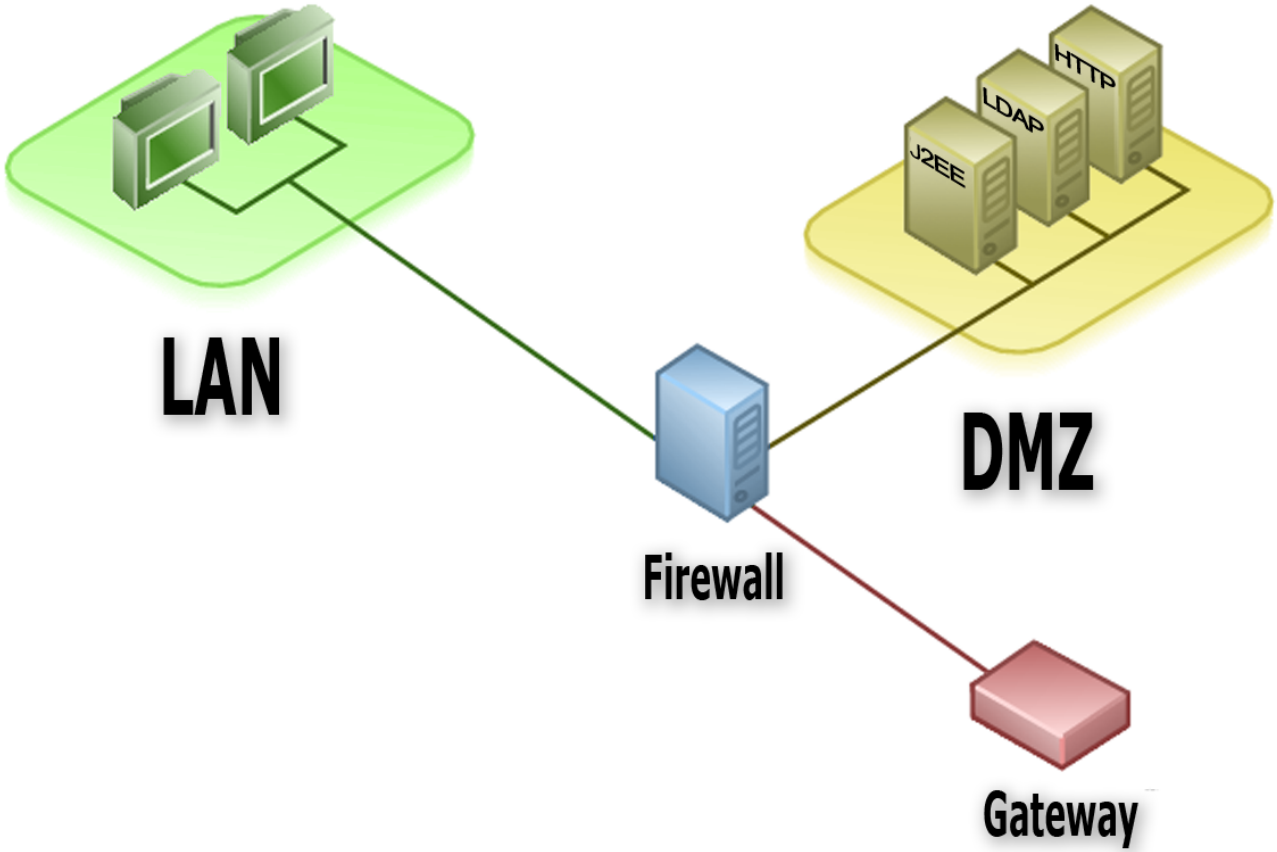
- Security Devices;
  - Dummie configs
  - Your needs
  - Not smarts by default ☺
- Admins don't know about the security;
- Network Structure;

iBLISS

SAMPLES

Network Design

- DMZ



iBLISS

Network Design[1]

- Routers

iBLISS

Network Design[2]

- Why servers are not protected from users?
  - Like a DMZ, just the necessaries ports/services.
  - Hard work, but it worths!

iBLISS

Firewalls

- Rules applied for no reason;
- Once applied, forgotten forever;
- Analyze traffic? Why? It's easier a wide-open rule!

iBLISS

IDS/IPS

- Doesn't IDS stop the attack?? Really, I didn't know about that :P
- Do I have to see the logs?
- I installed an IPS, my system is full-protected!

iBLISS

NACs (NAC x NAP x others solutions?)

- Many vectors:
  - DHCP Policy ? Use Static IP.
  - Domain Policy? Just don't use it.
  - Quarantine Network? Explore it, maybe your gateway is the freedom! ☺

iBLISS

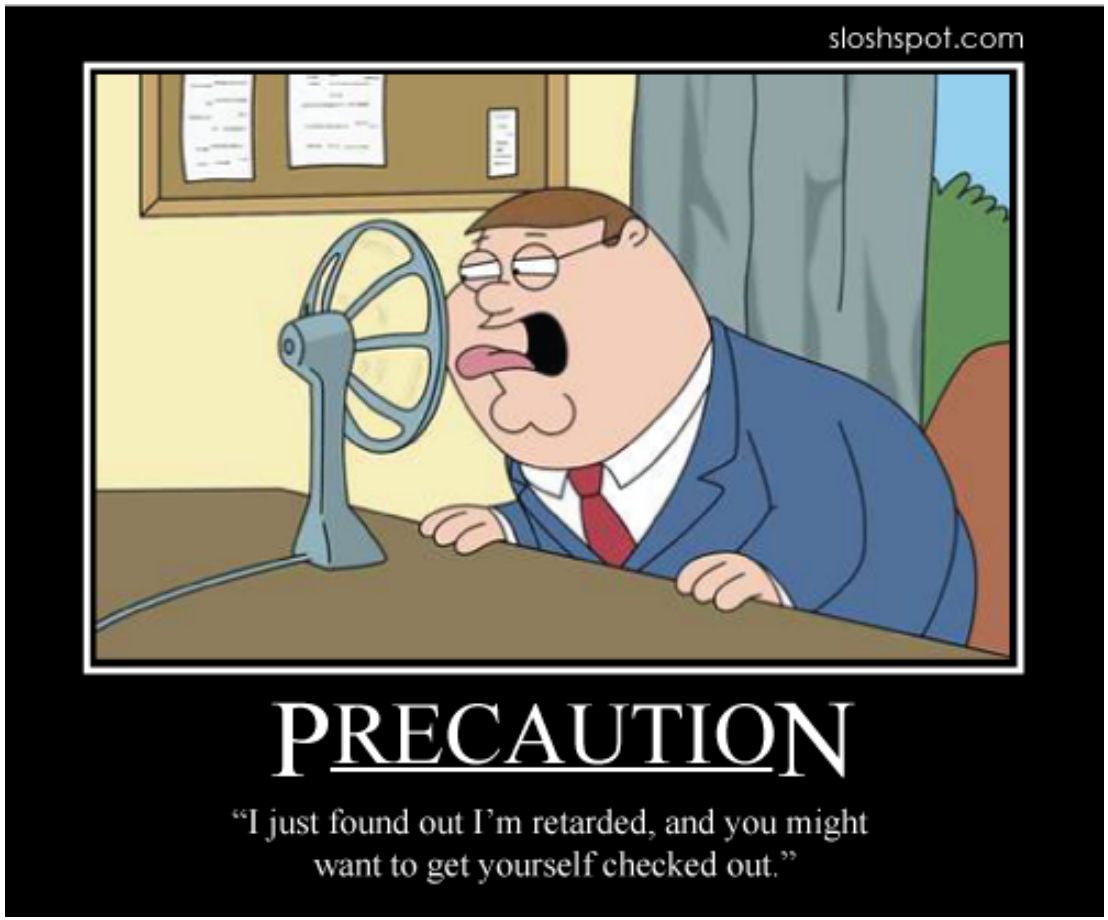
Social Engineer –What?

- Non-tech method to gather information;
- Persuade people do what you want;
- Can envolve technologie or not;

iBLISS

Social Engineer – Why?

- People SUX;
- People SUX[1];
- People SUX[2];
- People SUX[3];
- People SUX[4];
- People SUX[5];
- People SUX[6];
- People SUX[…];



iBLISS

Social Engineer – How?

- Get Familiar
- Create a hostile situation
- Gather and Use Information
- Get a Job There
- Read Body Language (like “Lie to Me”)
- HAVE SEX

iBLISS

TOOLS

- Metasploit ALL_TCP_Payloads;
- iPhone worm spreads via default password;

iBLISS

DEMO

- Social Engineer, for sure, is the most funny to show!
- Phone Call to a Big Company
- Authorized by the Company :P

iBLISS

The Call

- Get familiar with the person;
- ISP is easy to get, traceroute/dns/etc;
- Internet problems? Everybody has;
- CMD!
- People really sux! :D
- Open FTP (Local Network > Internet) | get malware.exe pwdump.exe
- Open SMTP (Spammer)
- Open POP3 (Just one more test)
- People really sux[2]
- SOCIAL ENG RULES!!!!!

iBLISS

Conclusions

- …
- …
- …
- …
- …
- …
- …

iBLISS

$ contact me

- bruno.mphx2 *nospam* gmail.com
- http://g0thacked.wordpress.com/
- http://blog.ibliss.com.br/
- http://linkedin.com/in/brunogoliveira
- #securityguys@irc.freenode.net
- hacking conferences around the globe
- parties, places with beer, etc…

iBLISS

iBLISS

ThankYOU!

Questions? I hope not.