Behind Enemy Lines

Hackmeeting 2009

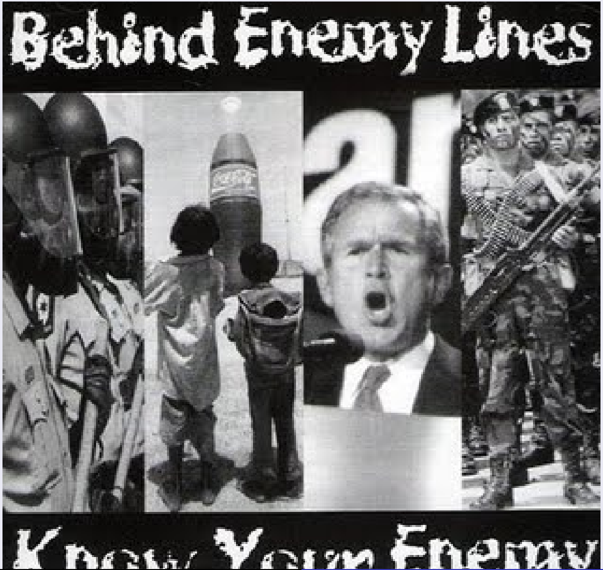
Dererk <dererk@buenosaireslibre.org>

Hack a Nice Day!

10, 11 y 12 de Octubre de 2009.

Topics

1. Cover
2. Being Behind Enemy Lines?
    - What's being Behind Enemy Lines?
    - Shape and get ready your tools and weapons
3. Know your enemy!
    - Size and meassure your enemy
    - Analyze their fenses
    - The strategy
    - Never understimate your enemy
    - Your enemies weakness
4. Some approaches about tools and weapons
    - The remote (home) sshd
    - An smarter approach
5. About this document...


Behind Enemy Lines
Know Your Enemy

Disclaimer

Why do you always refer to war, you bastards!

There are some situation in which daily events force us to take decitions about how to take our positions behind trenches and fortified fences. This time, we will be behind those fortified fences and trenches, what would you do?

When swapping roles...

- Chess Strategy: Make your moves with two steps beforehand!
- Play carefully: Patience is the master of techniques.
- 'Si pinta feo...'®: Soldier who run live for war.

When swapping roles...

- Chess Strategy: Make your moves with two steps beforehand!
- Play carefully: Patience is the master of techniques.
- 'Si pinta feo...'®: Soldier who run live for war.

When swapping roles...

- Chess Strategy: Make your moves with two steps beforehand!
- Play carefully: Patience is the master of techniques.
- 'Si pinta feo...'®: Soldier who run live for war.

When swapping roles...

- Chess Strategy: Make your moves with two steps beforehand!
- Play carefully: Patience is the master of techniques.
- 'Si pinta feo...'®: Soldier who run live for war.

Prepare your tools and weapons

- KNOW your tools and weapons!
- Be aware of your own weakness.
- Never ever doubt your weapons: A soldier who heasitate is a dead body.
- Trust your tools and weapons!

Prepare your tools and weapons

- KNOW your tools and weapons!
- Be aware of your own weakness.
- Never ever doubt your weapons: A soldier who heasitate is a dead body.
- Trust your tools and weapons!

Prepare your tools and weapons

- KNOW your tools and weapons!
- Be aware of your own weakness.
- Never ever doubt your weapons: A soldier who heasitate is a dead body.
- Trust your tools and weapons!

Prepare your tools and weapons

- KNOW your tools and weapons!
- Be aware of your own weakness.
- Never ever doubt your weapons: A soldier who heasitate is a dead body.
- Trust your tools and weapons!

Prepare your tools and weapons

- KNOW your tools and weapons!
- Be aware of your own weakness.
- Never ever doubt your weapons: A soldier who heasitate is a dead body.
- Trust your tools and weapons!

The big wall always has a catch

Analyze their defenses

Spend some time understanding them:

- Do they spend many time hardening their ENV?
- Are there any known vulnerabilities in their software?
- Do they exchange useful information over a easy-to-get media?

Analyze their defenses

Spend some time understanding them:

- Do they spend many time hardening their ENV?
- Are there any known vulnerabilities in their software?
- Do they exchange useful information over a easy-to-get media?

Analyze their defenses

Spend some time understanding them:

- Do they spend many time hardening their ENV?
- Are there any known vulnerabilities in their software?
- Do they exchange useful information over a easy-to-get media?

Analyze their defenses

Spend some time understanding them:

- Do they spend many time hardening their ENV?
- Are there any known vulnerabilities in their software?
- Do they exchange useful information over a easy-to-get media?

Prepare an strategy

Do not understimate them until they are already down on the floor, bleeding...

Some facts...

Your enemy is almost not ready to combat and less skilled than you, but never give anything as a fact

- Limited firewalling capacities for data mine every conection.
- Limited resources, in most cases (i.e. network security team).
- Limited time.
- Strategy plays in your favor!
- Surprise factor.
- KNOW your enemy!

Some facts...

Your enemy is almost not ready to combat and less skilled than you, but never give anything as a fact

- Limited firewalling capacities for data mine every conection.
- Limited resources, in most cases (i.e. network security team).
- Limited time.
- Strategy plays in your favor!
- Surprise factor.
- KNOW your enemy!

Some facts...

Your enemy is almost not ready to combat and less skilled than you, but never give anything as a fact

- Limited firewalling capacities for data mine every conection.
- Limited resources, in most cases (i.e. network security team).
- Limited time.
- Strategy plays in your favor!
- Surprise factor.
- KNOW your enemy!

Some facts...

Your enemy is almost not ready to combat and less skilled than you, but never give anything as a fact

- Limited firewalling capacities for data mine every conection.
- Limited resources, in most cases (i.e. network security team).
- Limited time.
- Strategy plays in your favor!
- Surprise factor.
- KNOW your enemy!

Some facts...

Your enemy is almost not ready to combat and less skilled than you, but never give anything as a fact

- Limited firewalling capacities for data mine every conection.
- Limited resources, in most cases (i.e. network security team).
- Limited time.
- Strategy plays in your favor!
- Surprise factor.
- KNOW your enemy!

Some facts...

Your enemy is almost not ready to combat and less skilled than you, but never give anything as a fact

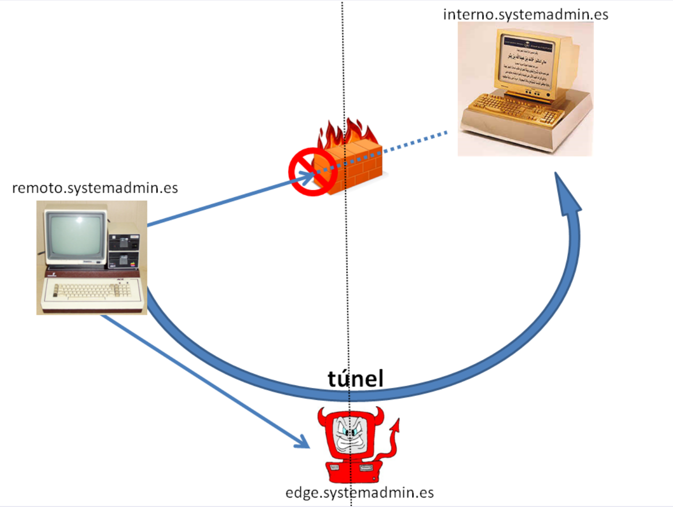
- Limited firewalling capacities for data mine every conection.
- Limited resources, in most cases (i.e. network security team).
- Limited time.
- Strategy plays in your favor!
- Surprise factor.
- KNOW your enemy!

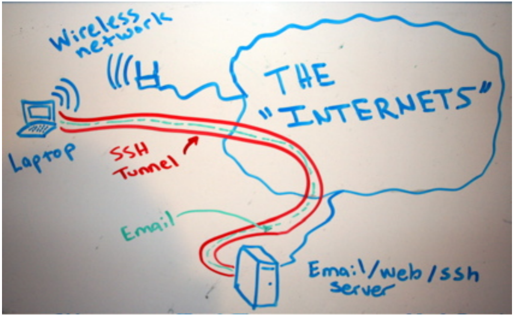
Some facts...

Your enemy is almost not ready to combat and less skilled than you, but never give anything as a fact

- Limited firewalling capacities for data mine every conection.
- Limited resources, in most cases (i.e. network security team).
- Limited time.
- Strategy plays in your favor!
- Surprise factor.
- KNOW your enemy!

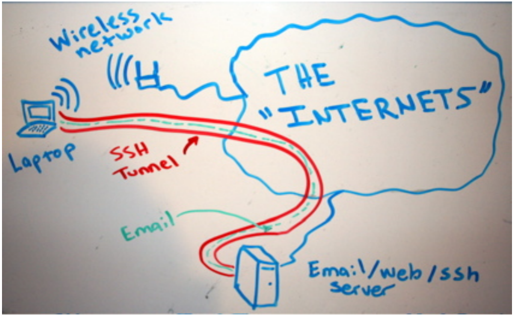
Hey! That one is easy!





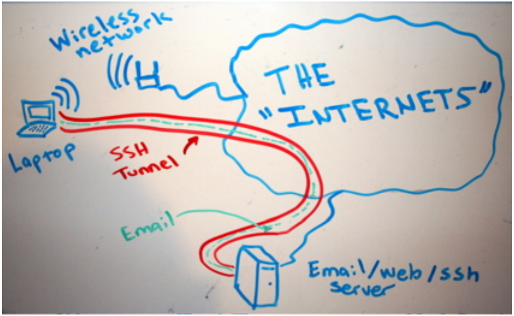
The remose sshd... uhm...

- A remote sshd somewhere and that's all!
- Uhm.... Ok, not outcoming 22 port...What's up now?
- Hey you! What about another port???
- OK, OK! NO open ports, except from 80 and 443... damn you!



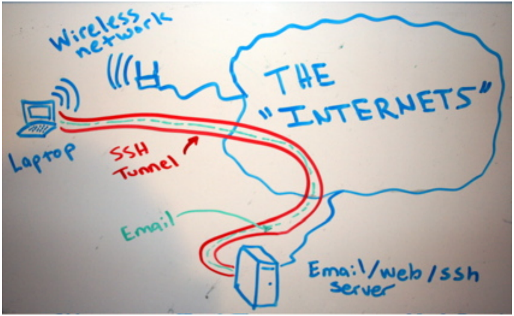
The remose sshd... uhm...

- A remote sshd somewhere and that's all!
- Uhm.... Ok, not outcoming 22 port...What's up now?
- Hey you! What about another port???
- OK, OK! NO open ports, except from 80 and 443... damn you!



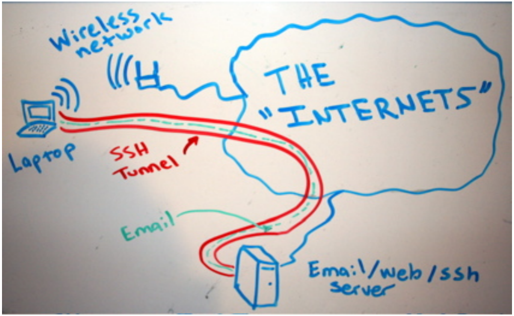
The remose sshd... uhm...

- A remote sshd somewhere and that's all!
- Uhm.... Ok, not outcoming 22 port...What's up now?
- Hey you! What about another port???
- OK, OK! NO open ports, except from 80 and 443... damn you!



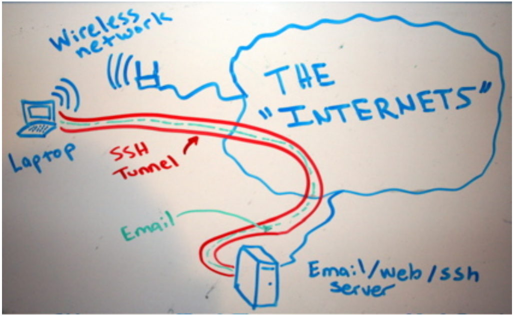
The remose sshd... uhm...

- A remote sshd somewhere and that's all!
- Uhm.... Ok, not outcoming 22 port...What's up now?
- Hey you! What about another port???
- OK, OK! NO open ports, except from 80 and 443... damn you!



The remose sshd... uhm...

- A remote sshd somewhere and that's all!
- Uhm.... Ok, not outcoming 22 port...What's up now?
- Hey you! What about another port???
- OK, OK! NO open ports, except from 80 and 443... damn you!



The remose sshd... uhm...

- A remote sshd somewhere and that's all!
- Uhm.... Ok, not outcoming 22 port...What's up now?
- Hey you! What about another port???
- OK, OK! NO open ports, except from 80 and 443... damn you!

The sshd approach, second chance, the proxy approach

Corkscrew, an https cheater!

- Smart approach for proxing SSH xtions.
- Modified HTTP CONNECT header.
- Randomize local ports to fake the HTTP proxy.

The sshd approach, second chance, the proxy approach

Corkscrew, an https cheater!

- Smart approach for proxing SSH xtions.
- Modified HTTP CONNECT header.
- Randomize local ports to fake the HTTP proxy.

The sshd approach, second chance, the proxy approach

Corkscrew, an https cheater!

- Smart approach for proxing SSH xtions.
- Modified HTTP CONNECT header.
- Randomize local ports to fake the HTTP proxy.

The sshd approach, second chance, the proxy approach

Corkscrew, an https cheater!

- Smart approach for proxing SSH xtions.
- Modified HTTP CONNECT header.
- Randomize local ports to fake the HTTP proxy.

What's wrong with the sshd tunneling approach?

The netadmins KNOWS who you're talking to!

- The netadmin or any cab®on in the middle can block you, BAD!
- The UFASTA/Citefa sshd threshold banner analyze! (.AR rulz, BAD sshd randomization) ;-)
- SO? WHAT'S UP TO DO!?

What's wrong with the sshd tunneling approach?

The netadmins KNOWS who you're talking to!

- The netadmin or any cab®on in the middle can block you, BAD!
- The UFASTA/Citefa sshd threshold banner analyze! (.AR rulz, BAD sshd randomization) ;-)
- SO? WHAT'S UP TO DO!?

What’s wrong with the sshd tunneling approach?

The netadmins KNOWS who you’re talking to!

- The netadmin or any cab®on in the middle can block you, BAD!
- The UFASTA/Citefa sshd threshold banner analyze! (.AR rulz, BAD sshd randomization) ;-)
- SO? WHAT’S UP TO DO!?

What's wrong with the sshd tunneling approach?

The netadmins KNOWS who you're talking to!

- The netadmin or any cab®on in the middle can block you, BAD!
- The UFASTA/Citefa sshd threshold banner analyze! (.AR rulz, BAD sshd randomization) ;-)
- SO? WHAT'S UP TO DO!?

The UDP tunneling approach

Iodine, the UDP DNS cheating tunneling aproach

- Iodine lets you tunnel IPv4 data through a DNS server, even over IPv6.
- Random DNS subdomain inquires.
- Strong crypto.
- Password-based authentication.
- Password-derived algorithm for randomization seeding.
- Available for BSD and Linux, and others ;-)

The UDP tunneling approach

Iodine, the UDP DNS cheating tunneling aproach

- Iodine lets you tunnel IPv4 data through a DNS server, even over IPv6.
- Random DNS subdomain inquires.
- Strong crypto.
- Password-based authentication.
- Password-derived algorithm for randomization seeding.
- Available for BSD and Linux, and others ;-)

The UDP tunneling approach

Iodine, the UDP DNS cheating tunneling aproach

- Iodine lets you tunnel IPv4 data through a DNS server, even over IPv6.
- Random DNS subdomain inquires.
- Strong crypto.
- Password-based authentication.
- Password-derived algorithm for randomization seeding.
- Available for BSD and Linux, and others ;-)

The UDP tunneling approach

Iodine, the UDP DNS cheating tunneling aproach

- Iodine lets you tunnel IPv4 data through a DNS server, even over IPv6.
- Random DNS subdomain inquires.
- Strong crypto.
- Password-based authentication.
- Password-derived algorithm for randomization seeding.
- Available for BSD and Linux, and others ;-)

The UDP tunneling approach

Iodine, the UDP DNS cheating tunneling aproach

- Iodine lets you tunnel IPv4 data through a DNS server, even over IPv6.
- Random DNS subdomain inquires.
- Strong crypto.
- Password-based authentication.
- Password-derived algorithm for randomization seeding.
- Available for BSD and Linux, and others ;-)

The UDP tunneling approach

Iodine, the UDP DNS cheating tunneling aproach

- Iodine lets you tunnel IPv4 data through a DNS server, even over IPv6.
- Random DNS subdomain inquires.
- Strong crypto.
- Password-based authentication.
- Password-derived algorithm for randomization seeding.
- Available for BSD and Linux, and others ;-)

The UDP tunneling approach

Iodine, the UDP DNS cheating tunneling aproach

- Iodine lets you tunnel IPv4 data through a DNS server, even over IPv6.
- Random DNS subdomain inquires.
- Strong crypto.
- Password-based authentication.
- Password-derived algorithm for randomization seeding.
- Available for BSD and Linux, and others ;-)

About this document...

This document was produced completely under LaTeX
The last modification of this document was done on 12 de octubre de 2009 and is released under CreativeCommons BY-SA 3.0 Unported license.