RED TEAM

redteams.net

TOC

The mindset

Be aware of your surroundings

The Adversary

Do you have a plan?

The “Team”

Going beyond

The mindset

A Red Team is a group of highly skilled people that continuously challenge the plans, defensive measures and security concepts.

But, what *is* a Red Team.

The mindset

A Red Team views a problem from an adversary perspective.

A Red Team can solve problems through an indirect and creative approach, using reasoning that is not immediately obvious and involving ideas that may not be obtainable by using only traditional step-by-step logic.

The mindset

Adversaries don't play by the same rules as the good guys. In fact they don't have rules at all.

They adapt.

The mindset

A Red Teamer plays with the different sides of the problem as if it were a hollow cube: you have the 6 external sides to check, yet you can't forget the 6 internal sides.

The idea here is to go beyond the visible, the obvious, and check also the extra things that no one has bothered to test before.

The mindset

"Red Teaming Law #11: The superior red teamer discerns webs of perception, intent, and effect; others just see a cigar. Of course, 'sometimes a cigar is just a cigar' (or is it?)"

-- Red Team Journal

Be aware of your surroundings

Adversaries can and will exploit any and all known attack vectors. They will also create new ones.

Attackers are very creative. Especially when they are motivated.

Be aware of your surroundings

Systems will be compromised. Perimeters will be breached.

You can’t just throw money at the problem.

Be aware of your surroundings

Is everything as it appears to be?

Really?

Be aware of your surroundings

Defenders often are so focused on the systems they want to protect, they forget one very basic truth…

Be aware of your surroundings

Attackers are extremely good at exploiting the human factor.

Be aware of your surroundings

"Amateurs hack systems,
professionals hack people."

-- Bruce Schneier

The Adversary

The modern enterprise is too complex for any individual or group to thoroughly understand how it can be compromised.

Adversaries know this. They thrive in this. They play with this.

The Adversary

Again: adversaries don't play by any rules. Attackers adapt and learn from their failures.

A good Red Teamer, then, has to adapt and play by the same rules of the adversary. In other words: no rules.

The Adversary

"To become the enemy,
see yourself as the enemy
of my enemy."

-- Musashi

The Adversary

Security plans and strategy sometimes are governed by what worked in the past and not on the dynamic world of the attackers.

Unless trained to think differently, a lot of the security professionals have a very well defined plan of action based on the past and on lists that other security professionals created.

The adversary doesn't care about the past.

Do you have a plan?

Do you? Good.

Now, forget about it.

(well, unless it's an escape plan…)

Do you have a plan?

The key here is attitude.

There is a reason for PACE: Primary, Alternate, Contingency, Emergency.

Again, thinking like an adversary. Adapting. Being everywhere and nowhere.

The “Team”

Building a Red Team is not an easy task. Having the right people *with* the right mindset is a hard problem.

The key of a good Red Team is adaptability and the ability to walk in the adversary’s shoes.

The “Team”

The first thing to know, to understand, is the individuals that comprise your team. It is a team, but without its members a team is not much of anything.

Each member has a specific strength. It is crucial to understand this, but more importantly, it is imperative to understand his/her weaknesses.

The “Team”

You don’t need a big team to be successful. You need the *right* team for that.

Often, the right team is a small team. A team able to adapt fast, think on their feet and overcome obstacles.

There is a reason for SOF teams to remain small and agile.

The “Team”

A small team, comprised of the right people, communicates better, acts and reacts smoother and provides cleaner ideas.

Going beyond

So, you have a Red Team. Now what?

Deploying a Red Team takes understanding of *what* a Red Team is. Not all managers/directors/commanders know what the Team can do or the benefits of having a Team.

A good Team Leader has to be able to communicate this.

Going beyond

Red Teaming has to happen constantly. The Team has to be engaging targets all the time. The perimeter, the systems, the plans. A good Team should be constantly developing attacks on the 3 main fronts: physical, digital and social.

Going beyond

Red Teaming is a dynamic process, it is a ongoing process, it is real life scenarios.

Make it count.

Remember:
When in doubt, Red Team it.

Thank you.