

RED TEAM



Digital Recon

redteams.net

So, you managed to social engineer your way into the network with full control of a system with admin level access.

Now what?

First things first. What is your target?

What are you after?

Data?

A specific computer or server?

A specific person?

Total disruption of the network?

Stop, look and listen.

Stop:

The defenders know their network better and have more visibility into everything than you do.

Keep this in mind.

Look:

See what's connected to the system you breached. Where can you go from there.

Listen:

Sniff the network. Try to get credentials. Try to learn what normal traffic looks like.

Now... It's all about data.

Files. Emails.

Porn.

Use drones

Record sound

Grab video

It's all about the exfil

Have a plan

Have a backup plan

Have an escape plan

Remember:
When in doubt, Red Team it.