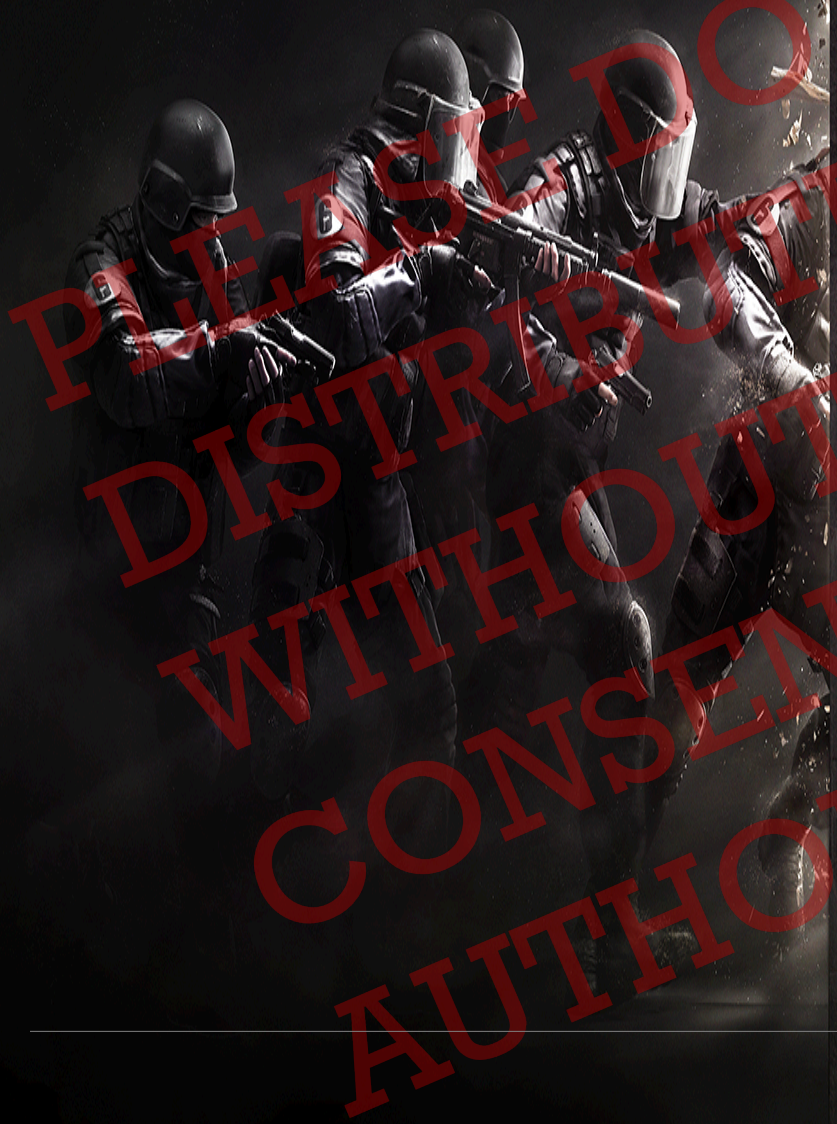


WHAT IS A RED TEAM



PENTESTING

IS NOT

RED TEAMING

RECENT EXAMPLE

Good intelligence

She said torture did not elicit the information that ultimately led to bin Laden. Instead, she attributed the operation's success to painstaking work by a rejuvenated intelligence apparatus that has moved beyond its failures during the Iraq war.

"It was a masterful job of intelligence," Feinstein said. She praised the Obama administration for making a "very gutsy call and go in. They could have sent a Predator (drone) with Hellfire missiles and killed everyone in the place. They didn't do it."

She pointed specifically to a technique called "red teaming" that tests and retests all available information for weaknesses or potential inaccuracies.

That was not done, Feinstein said, during the analysis that falsely assumed former Iraqi dictator **Saddam Hussein** had weapons of mass destruction, which provided the basis for the Iraq invasion in 2003.

<https://www.sfgate.com/news/article/Bin-Laden-data-not-had-by-torture-Feinstein-says-2372809.php>

Roei Sherman

♠ Red Team @  AB InBev

♠ Co-organizer @  BSIDES TLV

♠ OSCP, GPEN, GXPN, CCSK – SANS Advisory Board



<https://betheadversary.com>



x_Freed0m



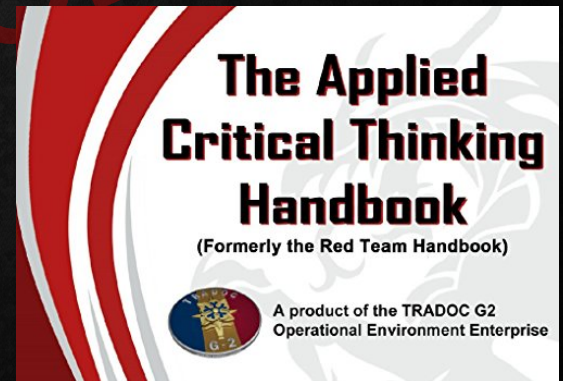
<https://github.com/xFreed0m>

PENETRATION TESTING

- ▶ Specific part of the system\organization
- ▶ Doesn't consider implications on other systems
- ▶ Doesn't test detection\prevention capabilities
- ▶ Aiming for as many findings as possible
- ▶ Focusing wide, not deep

WHAT IS RED TEAM ORIGINS

- ▶ “an *independent* group that challenges an organization to *improve* its effectiveness by assuming an *adversarial* role” (Wikipedia)
- ▶ The “what will go wrong” guys
- ▶ Started in the army
- ▶ Also used for business purposes, not only cyber



WHAT IS **RED TEAM** CYBER RELATED

- ▶ Not pentest on steroids
- ▶ **Red Team** is about challenging security posture
- ▶ Simulate **real world where possible**
- ▶ Aiming at specific objectives
- ▶ Will use all possible vectors*
- ▶ 1st priority is teaching the blue team/SOC & “winning” comes 2nd

DIFFERENT RED TEAMS

External

- Different environments\industries
- Can't control the members and their expertise
- Shorter engagements (or more money)
- Can be rotated between assessments

Internal

- Better familiarity with the environments
- Team can be shaped by the organization
- Cheaper to hire - expensive to train
- Already familiar with previous findings

PLANNING A **RED TEAM** ASSESSMENT

- ▶ What are your crown jewels?
- ▶ Who are the bad guys you want to simulate?
- ▶ Do you have buy-in from the stakeholders?
- ▶ Can it be kept secret?
- ▶ Are you ready to act on the results?
- ▶ White carding the limitations

THE PHYSICAL & HUMAN

- ▶ Physical entry
 - ▶ Picking locks
 - ▶ Bypassing doors
 - ▶ Disguising as personnel
- ▶ Humans
 - ▶ We know that's the weakest link:
 - ▶ Do we understand how weak is it?
 - ▶ How secure they are outside of your perimeter?

RED TEAM VS. PENTEST

Red Team


Penetration testing

- Going for objectives
- All vectors are valid
- Testing detection & prevention
- Zero-knowledge start
- Testing the organization posture
- Going for coverage
- Staying in scope
- Testing the component
- Walkthrough by the business
- Testing the component posture

PENTESTING IS NOT RED TEAMING



 <https://betheadversary.com>

 [x_Freed0m](#)

 <https://github.com/xFreed0m>