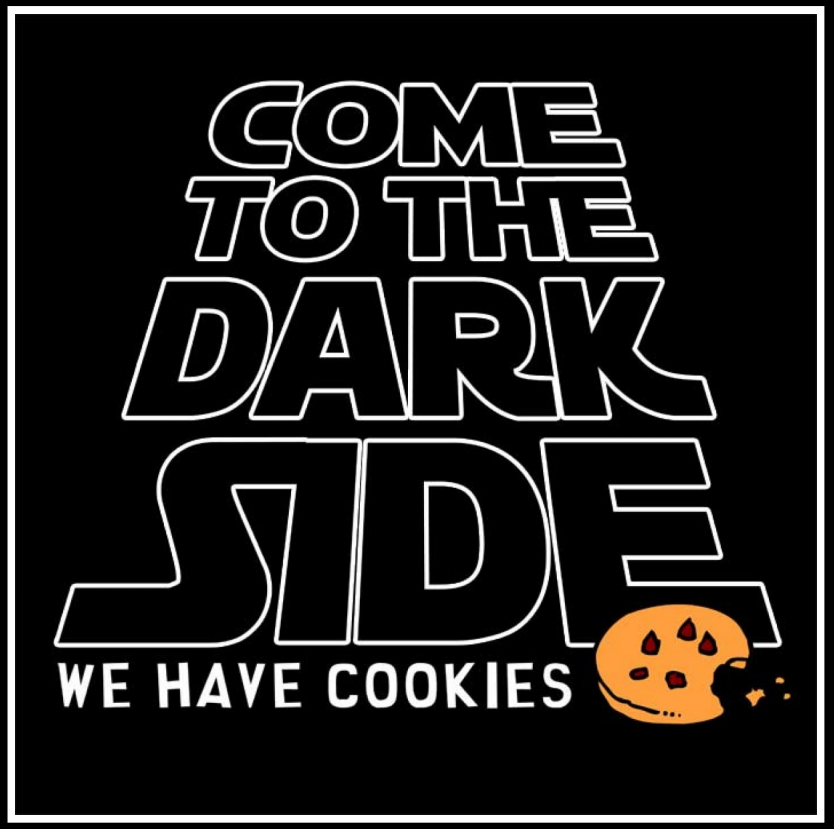


AN INVITATION TO OFFENSIVE SECURITY

WHOAMI

- @buherator
- ex-BuheraBlog
- CrySys dropout :)
- Silent Signal (2010 -)

GOALS

- Demystification
- Pointers to start
- Advice to progress

THE TRAINING

THE LOST WISDOM

Many believe that principles of offensive thinking can't be taught

- Breaking the rules
- Gaining power from chaos
- Disobeying restrictions

The Force within one seems to be of great importance

TRAINING

- Well tested methodologies are rare
- Technology changes by the day
- Reliance on undocumented workings

TRUE MASTERS KNOW

"breaking" is in fact "using"

"chaos" is just a barrier of your understanding

"restrictions" are tools in the right hands

TRAINING

- Fighting with complexity
  - Rational planning
  - Managed processes
  - Professional implementation

Formal education is gaining importance[#thoughtleading]

SCIENTIFIC APPROACH

- Reproducibility (e.g. BROP vs. BROP)
- Evidence based approach
- Clear definitions, understanding of possibilities

KNOW YOUR STUFF!

- Computer architectures (5 Galactic Credits)
- Operating Systems (4 Galactic Credits)
- Basics of Programming I-II. + SW labs (~12 Galactic Credits)
- Computer Networks (4 Galactic Credits)

THE BEST STAR-PILOT IN THE GALAXY, AND A CUNNING WARRIOR

- Learn to fly a T-16!
- Program some moisture vaporators!
- Clean and repair broken droids!

Then you can go for a security job

MEANWHILE...

DAMN VULNERABLE X

- Hologram machines designed by that traitor Galen Erso
- Best for beginners who can't force choke an Ewok
- Don't cheat!

BUG BOUNTIES

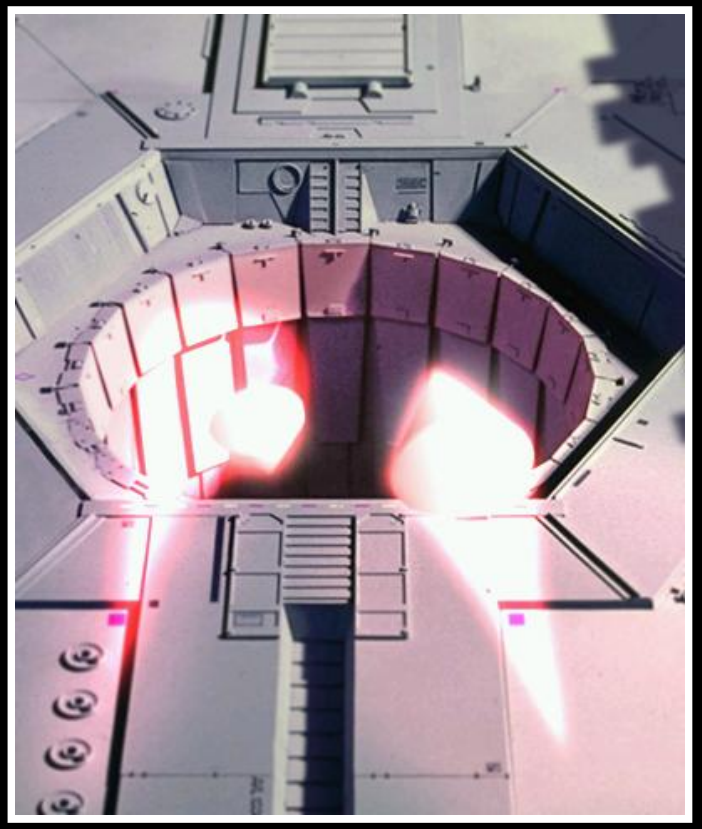
- Approved by the Empire
- Real systems to 0wn
- Tools & Techniques
- Scoping, reporting
- $$$

CTF

- Competitive environment
- Focused work
- Team work
- Tools & Techniques
- Force Learning exercise

SERVING THE EMPIRE

PENETRATION TESTING



PENTEST

- Simulating Rebel activity in Empire systems
- Presenting results to the Executive Branch
- Assistence with problem resolution

PENTEST

- Strong communication skills
  - In presence of Sith Lords
  - ...or Wookies
- Force Learning should be one of your top skills!
- And also...

READING MINDS

- Which part of this gate control was finished 2 minutes before Lord Vader arrived?
- What would Jar Jar Binks *assume* about this PHP type cast?

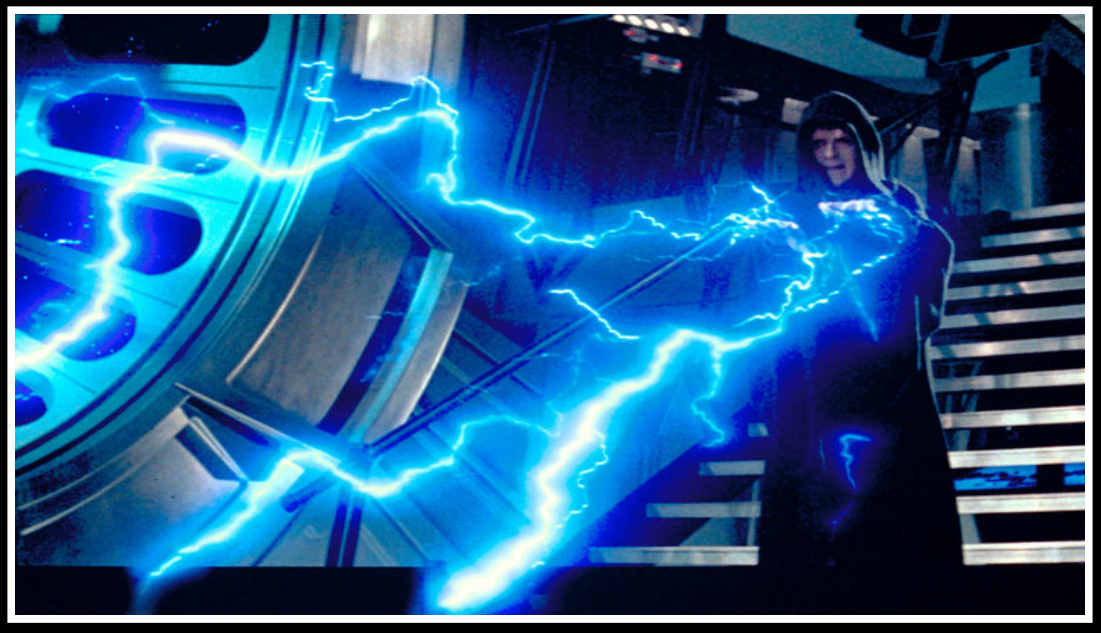
This is when experience with filthy droids and womp rats comes handy!

PENTEST > BUG BOUNTY

- Enforced methodology
- Definite targets
- Deeper insight
  - Intranets
  - Exotic technologies
- Assisting with issue resolutions
- Accountability

PENTEST > BUG BOUNTY

If rebels blow up the Star Destroyer you just audited with some proton torpedoes....



PROFESSIONAL BOUNTY HUNTING

SERVICE BOUNTIES

- Find new attack surface
  - Infrastructure discover
  - Feature discovery
- Find new attack techniques
- Can this be done reliably?
  - First strategy seems more fitting

SOFTWARE BOUNTIES

- Enterprise server software are a good start
  - Real impact
  - Usually riddled with critical holes
  - No/Basic mitigations
- Limited accessibility
  - Exclusive aquisition channels are valuable!

SOFTWARE BOUNTIES

Test environment Installation:

SOFTWARE BOUNTIES

High value targets

- Adobe Reader, MS Office, Death Star, etc.
- Sometimes with instrumented builds, fuzzing harness, etc.
- Strong shields
  - Exploit mitigations
  - Competition
  - Deprecation (e.g. click-to-play)

VULNERABILITY DEVELOPMENT

- RoT: Exploitation is ~10x harder than finding the bug
  - The actual ratio can be much worse than this
- Start easy
  - Known exploits
  - Known vulnerabilities

VULNERABILITY DEVELOPMENT

Imagine a CTF where

- The game lasts for months
- Writing an exploit can take weeks
- Not all targets have vulnerabilities
- Not all vulnerabilities are exploitable

So while playing CTF, pay attention to:

- Resource management (time, people)
- Attack surface identification
- Targeting (risk assessment)
- Team coordination

BECOMING

BECOMING

- Look beyond individual vulnerabilities
- Find ways that work universally
  - Or at least in multiple star systems
- The Empire demands results
  - Need for *practical* methods
  - In time

FIND YOUR PATHS

- Levels of abstraction
  - At low level many simple things work together
  - Higher level units encapsulate complexity and interact in "weird" ways
- It's worth figuring out the level you are most effective at

TOOLING

TOOLING

Exercise your skills by creating/improving tools

- Automation
- Proof of Concept
- Reproduction of prior results

TOOLING

We suck at this...

- Missing utilities
  - Create them!
- Low quality implementations
  - Fix them!
- Lack of documentation
  - Write them!

CONSTRAINTS

CONSTRAINTS

- Contraints no foolish Jedi can ovecome
  - Energy
  - Time
- Use these to make yourself powerful!

ENERGY

- The possibility of starvation can be a great motivator
- Fill up your reserves then go for it
- There is no try!
  - The little green dude was right about this...

TIME

- At the Academy, time seems infinite
  - And in some sense it is
- Make as much as you can out of this opportunity!
- Inclemency is key

TIME

- How long is a minute?
  - Ask someone held under the swamp of Dagobah!
- Planning
  - Sequence of short tasks (1-2h)
  - Goals within reach - Simple things that *work* (aka. KISS)
- Deadlines

COMMUNITY EVENTS

COMMUNITY EVENTS

- Idiots of the Trade Federation are taking over
- Throught the eyes of these fools
  - The powers of the Force are magic tricks
  - The Master is just a clown
- Don't let the lights and Jedi mind tricks blind your vision!

COMMUNITY EVENTS

- Look for teachers instead of rock stars
- Listen to content from (seemingly) distant fields
- Interact

LEARNING FROM MASTERS

- Do you understand the way it works?
- Can you do it yourself?
  - Show us!
- Can you improve it?

DEMONSTRATION OF POWER

- Prove yourself worthy
- Make your enemies fear & your allies respect you
- Empower the order of Sith
- meet deadlines...

THE DARK SIDE IS SEXY!

THE DARK SIDE IS SEXY!

- Discover yet uncharted parts of space
- Challenge the best minds of the Galaxy
  - ...whole armies even!
  - Conquer them for fame and fortune

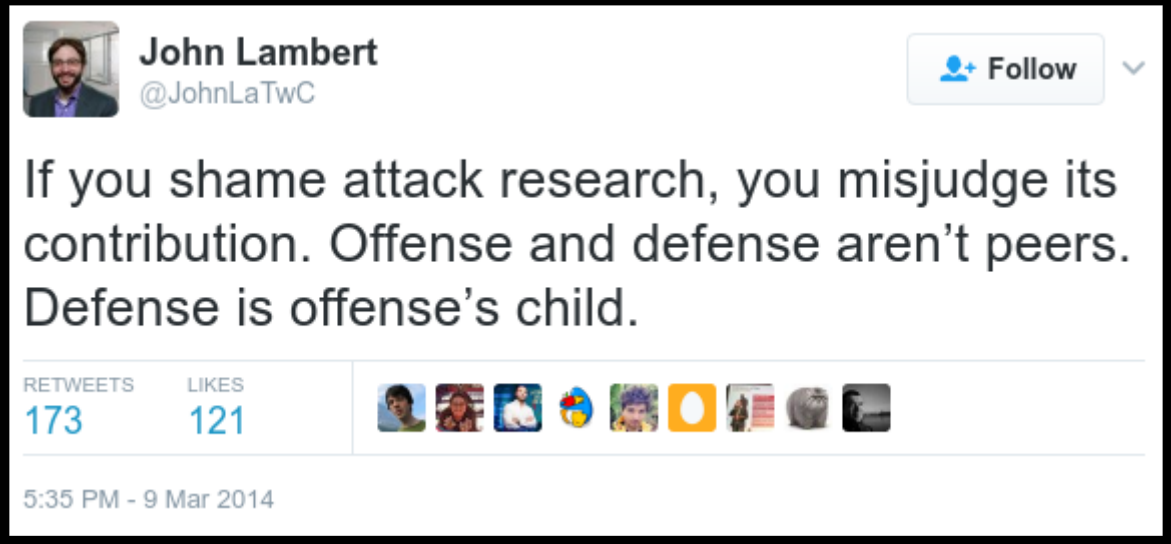
THE DARK SIDE IS POWERFUL

- The Senate just doesn't know what's going on
- The Light Side is paralyzed by ancient dogmas
- Mortals are terrible at making rational decisions

Eventually: The Sith will rule the Galaxy!

But in the end...

THE FORCE SURROUNDS US ALL



BEFORE LETTING YOU GO...

Questions?