siegecast:

PEN TEST PROCESS

PART 1: THE START

REDSIEGE
INFORMATION SECURITY

REDSIEGE
INFORMATION SECURITY

CONTACT:

+1.234.249.1337
contact@redsiege.com
@redsiege
@rsiege
/redsiege

OUR SERVICES:

ASSUMED BREACH ASSESSMENT

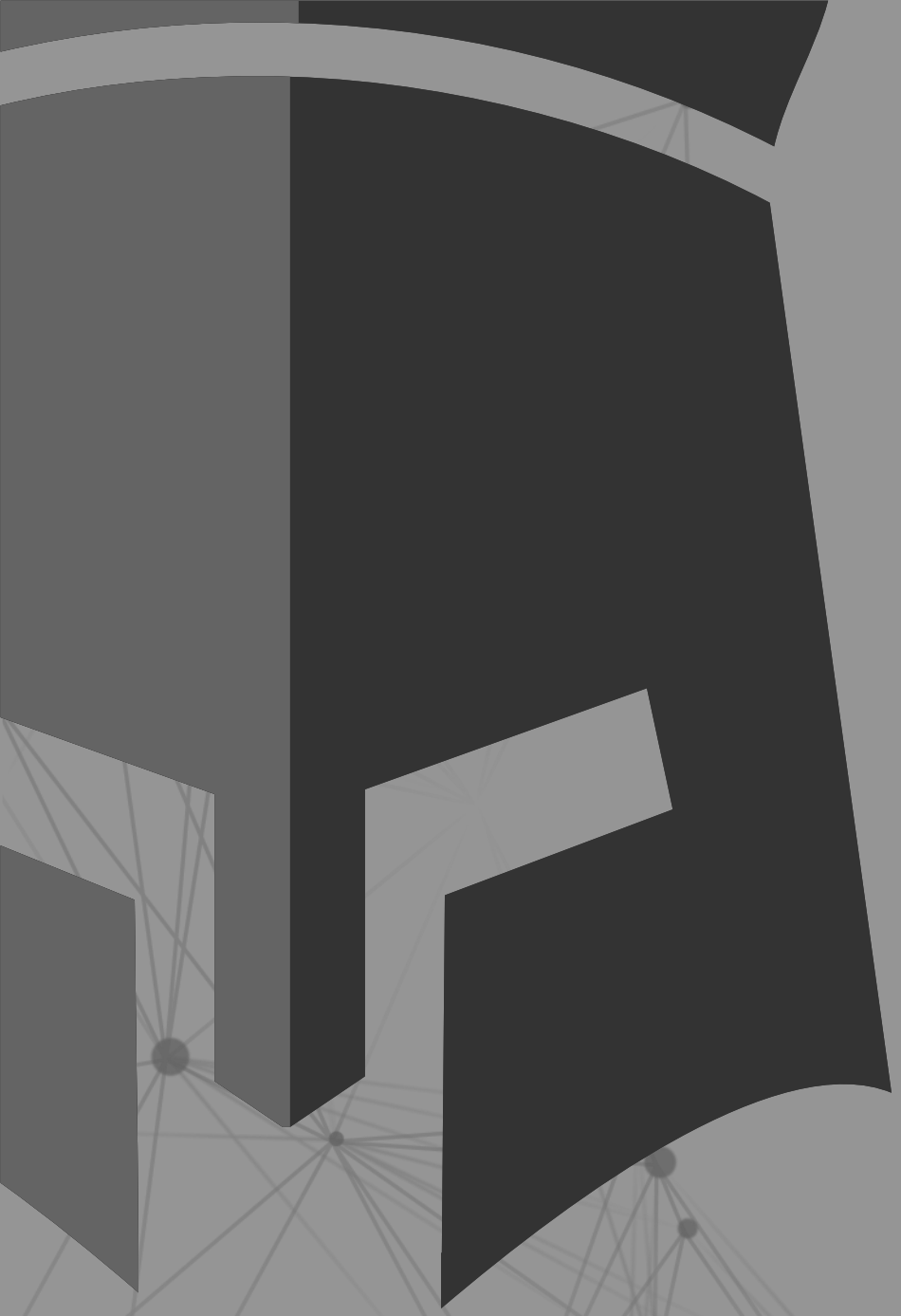
RED TEAM AND ADVERSARY EMULATION

PENETRATION TESTING

WEB APPLICATION PENETRATION TESTING

PURPLE TEAM

MOBILE APP ASSESSMENT



TIM MEDIN

Principal Consultant, Founder – Red Siege

SANS Leach Author – 560

SANS Instructor – 560, 660

IANS Faculty

Pen Tester for more than a decade

PEN TEST PROCESS

This is an excerpt of the material from SANS SEC560 (GPEN) where we cover the entire process of conducting a penetration test in an action packed 6-day course.
Tim Medin is the lead author of the "Network Penetration Testing and Ethical Hacking" course

A three-part series on pen testing

PART 1: THE START
PART 2: THE METHOD
PART 3: THE REPORT

AUDIENCE?

PEN TESTERS (INT AND EXT)
HIRING PEN TEST SERVICES
RECEIVING THE RESULTS

REDSIEGE
INFORMATION SECURITY

UNDERSTAND THE TARGET

- Testers: You need to work to understand the target to design a better test
- Testees: You need to understand yourself so you can steer the test and design
- Recipients: What do you want from the test? What kind of output?

Never assume! Ask the "obvious" question. State "the obvious".

A TEST IS ONLY AS GOOD AS THE PLAN

What are the biggest risks to the org?
You need goals

It does not do to leave a live dragon out
of your calculations, if you live near him.
J.R.R. Tolkien

REDSIEGE

BUSINESS RISK

GOAL FOCUSED

NEVER ASSUME

Ask the *dumb* question

"I can guess, but I don't like to be wrong, so can you describe for me what data or process if lost, destroyed, stolen, or leaked would cause the greatest damage to your organization?"

UNDERSTAND THE WHY

- Why is the test being done? Compliance? Improved posture?
- Who is the audience?
- What are the security goals?
- What are the security initiatives?

Understanding will help you tailor the test and test results

WHAT IS NEEDED TO TEST?

- Scope
- Types of tests
- Rules of engagement

The background information can help you define these and start the discussion on the most relevant topic first. Sometimes the test type is the first point, sometimes it is scope. It all depends on the goals and background information.

TEST TYPES

Organizational goals will define the test

TEST TYPES

- Internal Network
- External Network
- Assumed Breach redsiege.com/ab1 redsiege.com/ab2
- Egress & C2 testing
- Red Team
- Purple Team redsiege.com/purple
- Phishing
- Social Engineering
- Web App & API redsiege.com/webapi
- Mobile App
- Wireless
- Many others…

SCOPE

- What is in scope? – This determines time (and cost)
- What is out of scope?
  - Yes, this is the same question, but ask it too and you will get extra information
  - Why is it out of scope?
- What is owned by someone else?

WE WANT A REAL WORLD TEST

- "SolarWinds attack took more than 1,000 engineers to create"
  https://www.zdnet.com/article/microsoft-solarwinds-attack-took-more-than-1000-engineers-to-create/
- Attackers have a near infinite amount of time
- No one is going to pay an infinite amount of money*
- Set a realistic duration to get optimal results

*If you have an infinite amount of money, I like money. We should hang out.

RULES OF ENGAGMENT

- What can testers **do** without additional permission?
- What should testers **not do** without additional permission?
- Usually pretty simple, simple enough to be a simple list
  - Preapprove potentially more dangerous attacks, such as password guessing
  - All other "riskier" things need approval or a seatbelt

CAN THINGS GO WRONG?

Yes.
Systems crash on their own and there is an increased risk with atypical traffic

Does it happen all the time? No

Can it? Of course

Never guarantee 100% uptime, because no SLAs are 100%

Learn from mistakes redsiege.com/askus

OTHER THINGS TO PLAN

- Contact numbers for testers and target, including backups
- Secure communication methods
- Regular discussion times on longer tests

ROTATE TESTING ORGS

- IMO, this is a dumb idea that needs to die
- If you are getting what you want, then keep it!
- Example: If you go to your regular doctor, they have more background and can see longitudinally
- Maybe get different testers at the same org

This is not Tim saying use us only. If you never rotated, we never would have had work in the first place and would have gone out of business almost immediately. We exist because you rotated :)

THINGS TARGETS SHOULD DO

Some responsibilities will be solely (or largely) that of the target

IF YOU ARE THE TARGET

- Know what you want! (see earlier)
- Know your procurement process! If it takes 6 months for vendor onboarding, you need 6 months of extra lead time
- You can't just throw a pen test over-the-wall and expect a good test. Procurement people are great, but it isn't fair to expect they know all the technical details!
- Lead times are usually few months, Q4 is even longer!

IF YOU ARE THE TARGET (2)

- Ideally, this isn't a "throw it over the wall" kind of thing
- Contacts need to be available for outages, questions, or external compromise
- You know your vacation schedule!

THINGS TESTERS SHOULD DO

You have technical know how. You may need to guide the others.

IF YOU ARE THE TESTER

- Always be helpful
- You know the security issues better than anyone
  - Don't be a jerk
  - Put yourself in their shoes, think about their process

If the target doesn't improve their security posture, **<u>you</u> have been a waste of time**

Your job is to teach, not shame

We'll cover a lot more for the tester in Part 2 and Part 3

THINGS RECIPIENTS SHOULD DO

Some responsibilities will be solely (or largely) that of the target

IF YOU ARE THE REPORT RECIPIENT

- Ask for what you want ahead of time
  - Some orgs want data in a spreadsheet or CSV
- Does the sample report have the info you want or need?
- Use the pen testers!
  - Setup a debrief call to go through the report if you need it!

A three-part series on pen testing

PART 1: THE START
PART 2: THE METHOD
PART 3: THE REPORT

https://redsiege.com/pentestprocess2 (March 9th)
https://redsiege.com/pentestprocess3 (March 16th)

coming soon

WEDNESDAY OFFENSIVE

REDSIEGE
INFORMATION SECURITY

CONTACT:

+1.234.249.1337
contact@redsiege.com
@redsiege
@rsiege
/redsiege

OUR SERVICES:

ASSUMED BREACH ASSESSMENT

RED TEAM AND ADVERSARY EMULATION

PENETRATION TESTING

WEB APPLICATION PENETRATION TESTING

PURPLE TEAM

MOBILE APP ASSESSMENT