5 REASONS WHY AS A CUSTOMER...

...you are not getting value from pentests

YOU MAY NOT NEED A PENTEST AT THE START, BUT YOU STILL WENT AHEAD AND GOT ONE

- Resulting in thousands of vulnerabilities
- Instead, invest in a vulnerability assessment tool (like nessus, or nexpose). In many cases, Nessus may turn out cheaper than a pentest.
- Scan your environment, utilize internal vulnerability ratings by the tools
- Your infrastructure teams need to acclimatize themselves with closure of vulnerabilities, but most importantly,
- Your security teams need to learn to prioritize vulnerabilities
- Rinse, repeat for atleast 2-4 quarters/

NO ONE UNDERSTANDS PENTEST IN THE COMPANY, OR HOW TO MAKE MOST OF IT

- You need a top-down person in your team who understands the entire process of pentest (identifying what to pentest and what to keep 'out of scope', vetting the security reports before it goes up, getting risk assessment done on the findings, etc.), and a pentester who could help separate wheat from chaff (lack of security headers – is not always a 'high' vulnerability)
- Ideally, your security team should have both types of people. And no – one person seldom meets both criteria in equal measures.

WEAK RULES OF ENGAGEMENT...

- As a customer, you have every right to establish
  - List of DOs and DON'Ts
  - Expected outcomes (NO, it is not just part of red team; you have a right to know what you are getting into and what you will get out of it)

SECRET DESIRE TO PAY PEANUTS AND NOT GET MONKEYS…

- Good, cheap, fast – pick any two.
- Even a pentest company got to eat. They will put resources depending on the margins that they get. They can only bend so much without hurting them.

PASSING THE FINDINGS TO REMEDIATION TEAM WITHOUT PERFORMING RISK ASSESSMENT ON THE FINDINGS…

- Repeat after me – ‘pentest is not risk assessment’.
- What it means is – don’t cry wolf over every vulnerability. Not every vulnerability needs same attention. Decide which is the order of remediation. Risk assessment helps to do so.