Spilling the Beans: How to Spot a Bad Pentest

Andrew Clinton and Qasim Ijaz

Whoami

Andrew Clinton

- Director of Cyber Security at Aveanna Healthcare
- Former roles
  - Pentester, PCI-QSA, Security Architect, various sysadmin roles, etc…
- Creds
  - OSCP, OSEE, CISSP, …
- Focus areas
  - Security Leadership
  - Technical Risk Management
  - Security Program Management

Qasim Ijaz

- Director of Offensive Security at Blue Bastion
- Former roles
  - Sr. Manager Attack Simulation at Cigna, HIPAA/HITRUST Assessor at Meditology, etc.
- Instructor in after-hours
  - Blackhat, BSides, OSCP Bootcamp
- Focus areas
  - “Dry” business side of hacking
  - Active Directory exploitation
  - Healthcare security

Agenda

- The Client
  - How to evaluate security partners
- The consultant or consulting firm
  - Improvement ideas for your pentest practices
- Potential employee or candidate of consulting firm
  - How to evaluate employers

The Client: Your Goals

- Does your consulting firm understand what your goals are?
  - Did they listen to your needs and did they ask relevant questions?
  - Do they have flexibility to try to meet those goals.
  - Do they listen to you and understand what you do and what you need?
  - Do they make an effort to meet your needs/goals?
  - Does the SOW or contract reflect what you agreed on?

CAN YOU FINISH THAT IN A MONTH?
I CAN FAIL AT ANY SPEED YOU LIKE.

The Client: Flexibility to Meet Your Goals

- Do they have the skillset and flexibility to meet those goals
  - Do they have testers that are capable of giving you good results?
- Will the report reflect reality?
  - Does it show real impact?
- Andrew’s Story Time
  - This doesn’t fit our bucket.

The Client: Responsiveness and Project Management

- Do they have time for your project?
- Are they well organized?
- Will they have a dedicated project manager/coordinator for your project?
- Do they respect your time?
- Discuss timezones!!!

Ask for a Sample Deliverable

It’ll help ya!

Reviewing the Sample Deliverable: Good Report

- Impact based findings that consider effective risk
- Show impact but no FUD
- Break report into two sections
  - 1 section tailored to executives
  - 1 section tailored to technical teams
- Vulnerability scan is not a penetration test
- Prioritize your findings
- The report communicates the value of the testing

THAT'S WHAT I DO.
I DRINK AND I KNOW THINGS.
I'M A CONSULTANT!
made on imgur

The Consultant: Tailor To Client

- Understand the needs of your client and tailor the pentest to that including the report
    - Tailor the risk / severity to client's environment
    - Business drivers (why are they asking for an assessment)
    - Work with the client to make good use of assessment hours
    - Adjust communication to fit the client
    - Use the report to communicate the value of the assessment

The Consultant: Capabilities and Methodology

- Transparency with the client
  - Capability: If you can't do it, say so
  - Methodology: Don't hide how the work is being done
  - Communication:
    - Start/Stop emails
    - Activity summaries
    - Notification of high risk activity
    - Interesting findings.
- Transparency around timeline
  - Q's story time: Test concludes on Dec 31,
    - Go live on Jan 1st

DON'T WAKE ME I'M WORKING
I BELIEVE IT SAYS, "DON'T WAKE ME, I'M WORKING."

The Consultant: Price Transparency

- Transparency with the client
  - Don't hide the hourly cost, provide a breakdown
  - Don't fudge the hours spent or which tester is using the hours
- Did ya drop the price to compete?
  - Did you undercut the competetor and slash hours without telling the client?
- Andrew story Time
  - 'don't let the client know how the sausage is made'

The Consultant: Training and Culture

- Train your employees, do cross-training too
  - Pair up interested people with competent people in different skill sets in 1:1 skills
- Reduce the number of meetings that technical resources need to join
- Build a culture of collaboration, not competition

The Candidate: Interview Red Flags

- Legal documents
  - Overly restrictive NDAs or Non-competes
  - Andrew story - 3 year NDA
  - Andrew story - non-compete that kicks you out of the industry
  - Getting a sign-on bonus or restricted stock units? Read the agreement!
- Unable to meet with your future team and/or future manager
  - Interview process involves HR and senior leadership, but never gives you time with your future team or direct manager
- Lack of respect for your time
  - Not respecting the fact that you may need to take time off to interview
- Grilling the interviewee
- Asking questions only to show you “I know this stuff and you don’t”

The Candidate: Assessing future employers

- Outdated technology
  - Lack of cloud presence
  - Aging laptops
  - Mandatory onsite
- Reputation
  - What do your peers in the industry say about the company?
  - Check out Glassdoor, LinkedIn, and Twitter
    - Discord/slack channels
- What is their “billable” goal for you?
  - And how quickly do they expect you to achieve it?
- What does their Q4 look like?
- How often are consultants double or triple booked?
  - Andrew’s Story Time! PCI pentest over a weekend.

Conclusion

- Transparency
- Collaboration
- Honesty

Thank you!

Any questions?