To All CPTC Competitors:

As organizers of CPTC, our core goal is to foster education and help the next generation of offensive security practitioners gain practical experience that they can use in their future careers. To support this mission, we've been increasing the amount of feedback and information that we share with competitors in order to improve every team which participates in our event. Sadly, our time and resources are limited and not every team has the opportunity to make it to the final round of competition and experience all that CPTC has to offer, limiting that goal.

Broadly, reporting is one of, if not the single most important part of professional penetration testing. Our clients and customers are paying for our expertise, experience, tools, and techniques; however, the only lasting results we leave with them are their impression of our team and the documentation of issues: typically, our report.

Frustratingly this means that many different levels and parts of the organization are the targets of our reports; often with competing requirements. For example, a high level executive may look at deeply technical information incorrectly and get frustrated, worried, or have numerous questions that are outside their scope of expertise while a systems engineer often needs extensive detail to resolve an issue correctly. Reports need to be written for the Board of Directors, CIO, upper management, IT management, engineers, developers, risk managers, IT analysts, as just a few examples. Because of this you will often find multiple sections of a report attempting to aim for the needs of different groups.

Sadly, this also means that different groups will get confused by sections not meant for them. Different individuals will also give varying feedback based on their experience. This is also true when looking at CPTC scoring: one volunteer may grade something as a positive while others find it a negative. This is one of the most real-world aspects of the competition and is one of the main reasons we look for volunteers to score reports and presentations that are diverse in technical skill, organizational level, background, experience, and focus.

In our experience as professional penetration testers outside of CPTC, we also find this is an area almost all of our newest, least experienced team members struggle. Competing requirements and changes from team to team and client to client are an early career frustration for many, but over time they learn the art of report drafting that begins to balance these needs.

In the case of CPTC, there are some specific feedback and examples that we wanted to share based on our experience grading CPTC reports:

- **Do** include technical evidence that you were able to perform an issue. While this may be different in a professional setting, where you can have multiple deliverables, at CPTC you have one, and we need to be able to reperform what you've done or see that you've done it clearly.

- **Don't** include unredacted sensitive customer, employee, or intellectual property information in reports. Strive to aim higher than your client, who may have been terrible at storing information securely:

- **Do** include references to findings or relevant information to help your audience locate information and solve issues, such as technical links, example commands or code to fix the issue, etc.
- **Don't** use hyperlinks where without the full link, as reports are often printed or converted to PDF.
- **Do** use professional, third person, language and provide an explanation for everything you include, a screenshot on it's own doesn't communicate as much as one with context.
- **Don't** personally blame the client for any issues identified. Avoid second-person wording, such as phrases beginning with the word "you".
- **Do** include an executive summary, and make sure it's appropriate for the intended audience and level.
- **Don't** include excessive technical detail in an executive summary. This audience may not know what an IP address is, let alone care about it. This will often confuse the reader and cause more questions and concern than necessary.
- **Do** recognize that your client will have questions about your findings, and you will be asked to reperform some activities within client environments to validate their remediation. Clients that partner with you throughout the testing process are the clients you will want to work with year after year and are the ones that will often want to work with you.
- **Don't** just show the client how they messed up, show what they did well to give them some credit. A positive start can make a massive overall difference in how your message is received.
- **Do** always seek to learn and improve. The information security field is a relatively small, tight-knit community - and your reputation for quality work and integrity are incredibly valuable.
- **Don't** forget to proofread and spell check your report. These errors undermine your credibility and make your overall message less professional.
- **Do** provide reports in formats where they cannot be easily modified. Customers may want certain findings omitted from reports, but you should only document the resolution of these findings once they're remediated if you have validated the remediation and are still within the timeframe of your engagement. In general, findings should never be removed from a report as without the engagement they would have not been identified and resolved.
- **Don't** share your report with a client in an insecure way. Malicious actors would love to get their hands on one, documentation on all the weaknesses will save them effort..

Today, we're excited to announce another step to help competitors and the information security community as a whole: releasing all reports submitted for the International Finals event of the 2019 season of CPTC. While these reports have been anonymized to remove any remaining

team names and numbers, they represent the final deliverables from each team during this event. None are perfect, but are great examples for you to review to find the parts that you like the best. Every report, from CPTC to professional, is different. We look forward to seeing the new approaches you all have this year!

Thank you all for everything you do,

The CPTC Volunteers and Directors