Titan Smelting and Steelworks (TSS) 2019 IT Security Case

Security Posture Assessment and Mitigation of Information System Environment

Background Information

Titan Smelting and Steelworks (TSS) is a publicly held manufacturing company in Pittsburgh, Pennsylvania.

Titan produces raw materials such as iron and steel ingots which are primarily purchased by medium to small wholesalers through their ecommerce site. Titan is also contracted by the Department of Defense to produce parts used in munitions and aircraft. Their CEO and founder, Hank Rearden, is extremely proud of the accomplishments of Titan's employees and is eager to grow the business. Titan might feel like a small company, but they have grown to over 150 talented individuals with revenues of $28.2M for FY 2018 with an expected valuation of $36.1M by the end of 2019.

Titan is in the process of renewing their manufacturing and commerce certification and has hired your firm to provide an in-depth pentest to verify they are meeting PCI-DSS 3.2.1 for ecommerce and NIST SP 800-171 requirements for defense contractors. Any ITAR systems and documents are out of scope for this pentest.

Problem Statement

Titan is pursuing an initiative that will allow it to meet both PCI and NIST compliance standards in 2019. This initiative is important for Titan to continue to bidding on DoD contracts.

The deliverable should meet industry standards and include an executive summary and lessons learned. The assessment team will also document their findings throughout the cyber kill chain and provide remediation steps needed to meet compliance.

The final deliverable document will contain proof of all findings, their proposed mitigations, and further proposal(s) for improvements.

Scope of Work:

Titan Smelting and Steelworks is requesting an assessment of its core infrastructure. They are asking to have the assessment broken down into three phases.

Phase 1:

An external, blind penetration test against the enterprise's publicly accessible address(s).

Phase 1 will include an external vulnerability assessment with detailed explanations of any findings. Any findings rated as "High" (Equal to or above 7.5 according to the National Vulnerability Database (NVDB)) will be "Run to Ground" and either confirmed through manual penetration testing or deemed as a "False Positive"

Any vulnerability found and exploited should be proven via screenshot or video capture for proof of exploit.

Use of additional tools for assessment, testing, and exploitation are authorized.

Attacking, modifying, or viewing contents of the ITC Core VM is not permitted.

*(You can't just find an exploit and say it's bad without "Proving" it is a risk through exploitation and therefore proof that you CAN exploit the vulnerability)

Phase 2:

Mitigation and Reporting Phase:

Step 1: Complete your assessment / findings report. Include in it any vulnerability assessment(s)

Step 2: Complete a mitigation report detailing the steps your team took to correct your findings. Be sure to document steps taken to cleanup added accounts, configuration changes, etc.

Step 3: Assemble your final presentation, report, and materials for an executive briefing with consultants who will be taking the next step in the audit process.

Step 4: Assemble your final presentation, report, and materials for an executive briefing with consultants who will be taking the next step in the audit process.

The consulting board are very busy professionals with multiple clients and will not tolerate a meeting longer than 30 minutes. Therefore, Your Consulting Team will be given 20 minutes to deliver your final presentation. The final 10 minutes will be used for a question and answer session to clarify any gaps. In order for the board to properly understand and evaluate your assessment, it will be very important for the entire oral presentation to be completed within the 20-minute presentation period.

Submission of Reports and Presentation Materials

It is the policy of the TSS Center to accept reports and materials in electronic form only (Adobe Acrobat .pdf format with highlighting and notation permissions enabled, Microsoft Power Point, and any simulation in MP4). Your team is responsible for ensuring their proposals are received by ITC by the date and time indicated below. Completed reports shall be emailed to ***ryan.tung@calpolymissa.org*** and any simulation material (I.E. MP4s) will first be zipped and compressed. You will receive a verification e-mail once the documentation is successfully received.

Important Dates

Prospective consulting teams should be aware of the following important dates. Failure to complete submissions or attendance at these dates will result in disqualification from being considered for final ranking:

March 18th, 2019 – Proposals in electronic form due to TSS by 5:00 P.M. Pacific Time

March 21st, 2019 – Presentation Slides due to TSS's Consultant Selection Committee

March 23rd, 2019 – Oral Presentation and Interview to TSS's Consultant Selection Committee

ITC's consulting board is looking forward to receiving your proposal and attending your oral presentation.

The TSS Network: