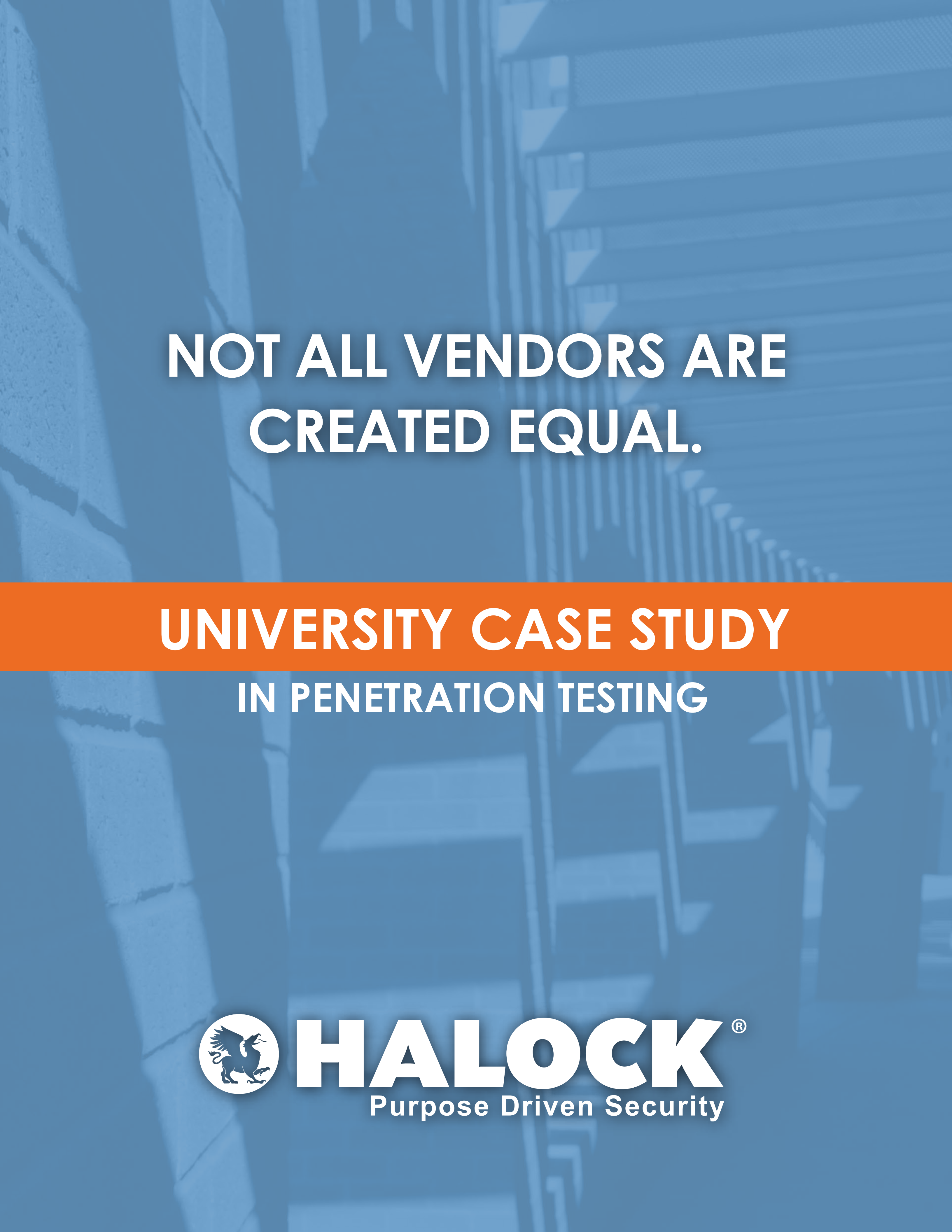

NOT ALL VENDORS ARE CREATED EQUAL.

UNIVERSITY CASE STUDY

IN PENETRATION TESTING

HALOCK®

Purpose Driven Security

BACKGROUND

A major university located in the Midwest was interested in comparing HALOCK's penetration testing services to those of a less expensive competitor to see if there were any material differences. The university manages more than: 15,000 students, 1,200 faculty members and 1,500 full-time staff members.

THE CHALLENGE

The goal of the web application penetration test was to determine how HALOCK performed, compared to the competitor, in a number of areas including quantity and accuracy of findings, quality and detail of deliverables, overall project management and efficiency, and test methodology. The university, which is budget-constrained, wanted to see if there really was a difference among penetration testing companies.

TEST PARAMETERS

The university requested a full web application penetration test rather than an automated vulnerability scan. With penetration testing, efforts are focused on exploiting weaknesses with the intent on gaining access to the application and connected systems. A vulnerability scan is an automated, low-cost method for testing common network and server vulnerabilities.

A detailed planning session was conducted ahead of the field work. HALOCK performed the web application pen test immediately after the other vendor so that results could be compared. After testing was completed, HALOCK detailed the findings and scheduled a meeting to discuss the results with the University.

At no time did the university share any of the findings from its original vendor before during or after the meeting with HALOCK. It was university IT staff, not HALOCK that conducted the comparisons between the reports of HALOCK and the other vendor.

THE RESULTS

HALOCK was invited to meet with the university information security team on campus to discuss the test results, recommendations, and comparison of the university's findings. The following table outlines the results.

	HALOCK	OTHER VENDOR
Quantity of Findings	12	6
Accuracy of Findings	All of HALOCK's findings were confirmed to be accurate by the university	Unconfirmed/Unknown
Format of Deliverable	Superior: Detailed, including images, complete with step-by-step infiltration scenarios, supported by screenshots on how to duplicate the exploits.	Adequate: Brief, text only.
Project Management & Efficiency	Well-managed, efficient, smooth process.	"A few grunts getting started, more of a learning curve." Too many people were involved. University was unclear who was managing the project.

Overall, HALOCK discovered twice as many vulnerabilities as the competition, including the utilization of cross-domain scripts and directory browsing. Utilizing cross domain scripts can allow attackers to easily find content that is intended for authorized personnel only. Directory browsing allows attackers to better fingerprint the underlying web server. The other firm's misses were deemed "disconcerting" by the university information security team.

> ***"I appreciated that your [HALOCK] staff also gave us the courtesy to know when you were beginning to test and when you were ending. The other vendor didn't even do that! It helped me, because when I saw unusual network traffic – I immediately knew it was the pen testing."***
>
> ***- University Security Operations Personnel***

The university felt that HALOCK's presentations, both written and oral, were superior to those of the other vendor. HALOCK presented a well-organized report of findings with vulnerabilities categorized with severity levels of high, medium, and low. Additionally, the report contained a detailed walk-through of the university's environment, including screenshots and examples, so that information security staff could easily understand the findings and supporting evidence. Finally, the university felt that HALOCK was very efficient and did a remarkable job project managing, while the other vendor had a lot of confusion, too many contact points and loosely defined testing timelines that contributed to university anxiety and confusion. The university felt overwhelmed by the other vendor's staff, often not knowing who was in charge, and who was managing the project.

> *"When I have a test done by HALOCK, it's done at a higher level. The other vendor's deliverables are missing key vulnerabilities, lack a thorough description of the vulnerabilities, and are just not as professional. You get what you pay for. Even HALOCK's presentation and discussion of the findings were superior to the other vendor."*
>
> *- Director of Enterprise Architecture & PMO*

DID YOU GET YOUR MONEY'S WORTH USING THE OTHER VENDOR?

A university IT Director responded, "For higher impact applications, I would be hesitant to use a cheaper vendor. HALOCK is definitely more thorough. I like HALOCK better – hands down! You get what you pay for!"

About HALOCK Security Labs

Founded on the strategy of "Purpose Driven Security", HALOCK Security Labs is a new breed of information security professional services firms combining strategic security consulting and compliance with technical security architecture and implementation. HALOCK services include Governance & Compliance, Technical Assessments, WorkForce, Incident Response, and Advanced Malware Threat Protection.

Purpose Driven Security®

HALOCK Security Labs has pioneered a new security model to meet these cyber threats. At the foundation of this new model is a service philosophy called Purpose Driven Security which helps define the right amount of security to protect critical assets; not too much, not too little. The philosophy can best be summarized as measured and preemptive risk management.

HALOCK®
Purpose Driven Security

For more information Contact Us:
847.221.0200 | info@halock.com | www.halock.com