Penetration Test Agreement

Jigar Patel
09/06/2023

Scope of Work

1. **Art's Tailor Shop** ("customer") (on **1 Tailor Shoppe Plaza, Kirkville, FL 32991)** CEO **Art Rosenbaum** has requested a **Black Box penetration/security test** on their computing & network infrastructure from Pr0b3 security (a HachiSec Company on **1 Pr0b3 Blvd, Hanksville, FL 33999)** in light of preparing to launch their web application.
2. The penetration tests will be performed for the period **09/06/2023** to **12/06/2023.**
3. The following are network domains and machines/routers that are in the scope of testing:
    a. **artstailor.com**
    b. **172.70.184.133/24 aka www.artstailor.com (Internet-facing web server)**
    c. **172.70.184.3/24 (Internet-facing router/firewall)**
    d. **3 WPA2-protected Wireless Access Points.**
4. In the case Pr0b3 security is able to breach the outer network, it has been **authorized** by the **customer** to **continue breaching** into the **internal network** by performing privilege escalations and lateral movement to maximize the visibility of weak points in the infrastructure by means such as password dictionary attacks, man-in-the-middle network attacks, social engineering, etc. Therefore the 6 **machines** in the **internal network** that are used by the CEO and various departments are also **in scope** for testing.
5. Pr0b3 security will **uphold industry best practices** while performing the tests and try to minimize any losses in the availability of machines and data during those tests.
6. Pr0b3 security will **not be liable** for any **damages** to hardware, software, data, and business operations that are direct or indirect results of the test.
7. Pr0b3 security will **not share or disclose** any **confidential information** about the internal infrastructure, business operations, or the results of the assessment with any **unauthorized third party**.
8. The tests **do not guarantee** that the **infrastructure is secure** from all kinds of compromises, as **Cybersecurity continuously changes and evolves**.

Rules of Engagement

1. The tests will be conducted remotely over a secure connection from Pr0b3 Security's main office at **1 Pr0b3 Blvd, Hanksville, FL 33999.**

2. The test window is all days of week, any time from **09/06/2023** to **12/06/2023 except** during **UF INFOSec team meetings** that are conducted every **Thursday from 6:00 PM** to **7:00 PM.** Pr0b3 Security will make its best efforts to be updated on any changes in those timings, however, it is the customer's responsibility to preemptively reach out to avoid any business losses.
3. Pr0b3 security will send weekly reports of progress on Monday by 3:00 PM or incident reports at their will to **Operations Manager Otto Oppenheimer** (on **opp@artstailor.com**) at **Art's Tailor Shop** using publicly available encrypted email communication such as Gmail or Outlook.
4. To **stop or temporarily pause** the tests, the customer can reach out to Pr0b3 Security's Point of contact **Hank Hacker** at hank_hacker@pr0b3.com or +1 352-999-XXXX during any hour of the day. Additionally, the customer can physically reach out at the aforementioned main office (**1 Pr0b3 Blvd, Hanksville, FL 33999**) address during business hours
5. Any **Social Engineering** attempts will be **preapproved** by the **CEO Art Rosenbaum**.
6. Any **data** from the customer's machine that will be copied to Pr0b3 Security's machines (whether it be for proof of concept or part of the attack such as passwords, Kerberos tickets, etc.) will be **stored in encrypted drives** (using state-of-the-art encryption standards such as AES) and only be **disclosed to authorized personnel only (**the pentesters who are assigned by Pr0b3 Security, and their direct managers**)**. Furthermore, after the submission of the final report, **all data will be deleted**.

The reasons for choosing these elements

1. Scope of Work
    1.1. The who's and why's for this test.
    1.2. Mentioning the general time period.
    1.3. Identifying the internet-facing domains, machines, and routers that will be tested.
    1.4. Mentioning that Art and Op said to breach deep into the network and thus get the internal machines into the scope as well.
    1.5. Clarifying the standards held by the firm.
    1.6. Protecting the firm from any unforeseen liabilities.
    1.7. Disclosure agreement.
    1.8. Protecting Pr0b3 Security from liabilities due to newly discovered attacks.
2. Rules of Engagement
    2.1. Mentioned that the communication channel that could be potentially transmitting sensitive data would be secure.
    2.2. Fine-grained time period with exceptions.
    2.3. Mentioned the frequency of communications between the firm and the customer.
    2.4. Provided the emergency contact to the customer.

2.5. Social Engineering agreement.
2.6. Data handling protocols that will be followed by the firm.