Social Engineering Penetration Testing

Emergent Research Forum papers

Thomas Arthur Talmadge
University of Maryland Global Campus
rickshaw98@hotmail.com

Executive Summary:

Human cybersecurity failures continue to be the major cause of data breaches. Social engineering takes advantage of these human failures; however, penetration testing strategies and methodologies have still not fully embraced socio-technical aspects of cybersecurity brought on by human failures.

1) A more holistic approach to penetration testing that embraces a multi-discipline approach with a social engineering focus helps.

2) The focus of cybersecurity in an organization must be aligned with the threat.

3) Efforts to model and standardize penetration testing and the effect on social engineering penetration testing also help. Social engineering itself can be an attack vector, can enable technical attacks, and or can identify vulnerabilities to exploit.

Time and again research shows that people are the biggest cybersecurity threat to an organization. Social engineering aspects need to be the primary focus of dynamic organizational penetration test strategies using standards and models to focus the social-technical penetration test efforts.

Keywords

Cybersecurity, Penetration Testing, Social Engineering, Modeling, White Box, Black Box.

Introduction: "The human factor is truly security's weakest link." (Mitnick, 2002)

Research and case studies of successful data breaches time and again show that the human factor is the "weakest link" in an organization's cybersecurity defense (Gyunka and Christiana, 2017; Mitnick, 2002; Mitnick 2011; Tischer, 2016; Whitman, 2003; Whitman and Mattord, 2010). Part of the issue is that the field of social engineering is so broad. There is a wide gulf between getting passwords and other sensitive data *just by asking for it* (Mitnick, 2002) and using extensive open source research to create a targeted spearfishing campaign with spoofed web pages (Wood, 2006) to extract information. As an example of the human challenge to cybersecurity defense, Tischer et al (2016) pointed out that people still plug in USBs found on the ground, despite this being one of the most common and basic warnings in organizations.

Penetration Testing Basics:

Midian (2002), a cybersecurity consultant, reminds IT practitioners that the first question that needs to be asked is, w*hat is the aim of the penetration test?* This is an important starting point for penetration test discussions because there are multiple uses of the methodology, which differ based on the desired end result. Further, Midian reminds organizations that from their point of view the answer should be to test the security of the target organization. But, this might be an oversimplification. There are multiple reasons for penetration testing and each organization will need to target their penetration testing. By definition, penetration testing is always an afterthought with Whitman and Mattord (2017) defining penetration testing as: a *set of security tests and evaluations that simulate attacks by a malicious external source (hacker).*

The most basic classification is black box testing, which assumes no insider knowledge, while white box testing is contrasted as having inside knowledge of the code or organization (Midian, 2002). From a holistic, simplified view these theoretically relate to external hackers (black box) and internal threats (white box). The challenge of this simplified view is that social engineering is a documented way to gain insider knowledge (Mitnick, 2002 and 2011) -- which can, in effect, turn a black box test into a white box test as a hacker methodically gains insider knowledge. Thus, finding the proper mix of white and black methodologies is a challenge for an organization. Specifically, in the NIST Technical guide to information security testing and assessment (Scarfone, Souppaya, Cody, and Orebaugh, 2008), there are a mere two paragraphs in this eighty-page guideline for cybersecurity security assessments which relate to social engineering penetration recommendations.

If each piece in the system is penetration tested, why test the overall system?

The actual organizational goal is also important, as hardware, software, and networking technicians each have cybersecurity penetration testing in their project cycle. Traditionally, these penetration test methodologies are technical in nature (Candell et al, 2014 and Tang, 2014) – it is not feasible for the software, hardware, networking engineer to know specifically the overall interaction between all systems and those systems with actual users. Federal workers with extensive recurring cybersecurity awareness training use the same Windows 2013 software tools as a home business individual on a laptop. By design penetration testing comes at the end of a process, but the actual software or hardware project is to create a product that **does** something and this traditionally comes prior to discussions on cybersecurity aspects. With the push for ever shorter project cycles to get hardware, software, and even complex IT systems implemented faster.

Tomanek and Klima (2015) discussed the challenges of implementing cybersecurity penetration testing into agile project methodologies, but also discuss an organization's penetration methodology: Is it enough to rely on each phase of the project's individual penetration testing? Or, does an organization then need to conduct overall penetration testing of the combined system? Tomanek and Klima (2015) concluded that while introducing penetration testing into the agile software development framework had several major advantages, there were additional costs and complexity for the required specialized automated technical penetration testing tools. This research is relevant because it identifies an existing challenge for software and hardware manufacturers with introducing standardized penetration testing into their project lifecycles, but also because it reinforces the methodology that we cannot rely on penetration testing each piece and assuming the whole is secure. Further, as each piece is created and tested in a technical vacuum, there is no way to introduce human cybersecurity vulnerability penetration testing into the design process.

Watson, Mason, and Ackroyd (2014) discussed the requirement for *blended assessments* for penetration tests in organizations and discuss social engineering taxonomy challenges- Do toolkits for targeted research to create an influence or situation to get someone to click on a technical attack link count as “social” aspects? Bishop et al (2010) discuss the idea of socio-technical aspects of cybersecurity, in relation to dealing with insider threats on an enterprise level. This work discusses the challenges of modelling human behavior in technical environments, as trust and other intangible issues are key to human cybersecurity behavior assumptions. Further, as motivation is the key discriminator for internal threats, there will always be a challenge with technical monitoring and prediction solutions for cybersecurity that focus on actions vice motivation. This provides a better framework for addressing the human cybersecurity risk. As this is also true in the opposite paradigm, is the caller/emailer to an organization motivated by getting their work done or for nefariously trolling for insider information to set up an attack? Thus, the same answer from a worker within the organization can either be normal daily operations or part of a larger cybersecurity scheme, but the action is the same.

Automating and Modeling Social-Technical factors:

Standardized models and penetration testing can be implemented on specific pieces of the system and models can be helpful for assessing unique characteristics for regulated or standardized systems. Candell, Stouffer, and Anand (2014) wrote for NIST identify standards for a cybersecurity test bed for industrial control systems, but this focused on manufacturing and technical cybersecurity without mention of penetration testing the final design. However, the design does provide insight into designing penetration tests. Similarly, Ahn, Chung, Min, and Seo (2015) proposed modeling nuclear power plant cyber-attack scenarios based on the inherent system designs and show that using scenario graphs provides cybersecurity personnel the ability to create realistic cyber-attack scenarios. These are examples of using system standards and modeling to enable cybersecurity planners vice relying on these tools to automate the process.

Penetration testing- What’s the Risk?

Within this wide gulf is also the overlap between social engineering and technical attacks. Bishop et al (2010) discussed cybersecurity against insider threats as a “socio-technical" or "cyber-physical-social systems" and Pieters (2011) expanded this to discuss modeling human interaction in system security. These discussions are applicable because they represent the challenges of combining human interaction with technical systems and the unique vulnerabilities that result. Thus, to fully realize cybersecurity, social, technical, and socio-technical aspects need to be addressed. Asking for the information (social) is part of the spectrum as well as the spearfishing campaign that relies on technical aspects (socio-technical). Pieters (2011) further expanded on the socio-technical research to create a cybersecurity model that introduces the human behavior variable into system security models. He discusses the challenge of internal threats in a way that also applies to social penetration testing and starts the modeling with basic questions:

1- Do indications for insider activity exist?

2- If there were an insider, what could s/he do?

These basic questions are also applicable to penetration test designs. On a continuum, they are directly applicable to white box testing, but also provide a worst-case scenario for black box testing. As social engineering moves the cyber-attack along this continuum from black to white to enable hackers, these basic questions also apply to the logical ultimate risk for any process that includes humans – all the capabilities of the targeted insider plus all those that that insider may influence.

Gyunka and Christiana (2017) discussed in their case study of the HBGary Federal security firm how once inside the company systems, through technical means, and the leadership emails were hacked the attackers used social engineering to gain additional root access into the systems. Thus, the technical systems worked, to a point, as the attackers ultimately wanted root access but were denied. So the attackers moved to social engineering by sending emails "from" the founder of rootkit.com to the chief security specialist that provided final access. Thus, the attacker used social engineering to work through the system to a worst-case scenario, which ultimately led to the demise of the entire HBGary Federal organization.

A better approach is to move to a multi-disciplined approach to penetration testing- Combining factors on the social to technical spectrum (Watson et al, 2014). But, this is more art than science. What made Mitnick great was his combination of technical and social attack methodologies artfully and seamlessly employed against an organization. Mitnick (2002, 2011) used technical attacks until he encountered a roadblock, then employed social attacks for the specific targeted information that he needed, then went back to technical attacks and, so on.

Conclusion- Social Engineering: We need the "Hacker":

Creating standardized penetration tests, based on modeling and standards, for individual pieces of a system is inherent and helpful for an organization to identify and target the most glaring deficiencies. However, these individual tests do not show the true extent of the risk to an organization, because they are based on the assumption that each works in a vacuum and that the risk is related to the reach of the individual piece of the system. The reality is that social engineering works within and across systems relying on the human weaknesses of the system, thus the actual risk is worst case for the most vulnerable individual system – social engineering provides a cross system and hierarchy threat. Models and standards can provide a framework for targeting penetration tests, but the actual penetration tests, being "art", must be completed by a human "hacker". Finally, the only way to fully test the interaction of all the elements within a system is through organizational enterprise social engineering penetration testing. This testing reality, along with the aspect of social engineering threats working across systems, combined and the research that continually shows that humans are the weakest link in the cybersecurity mechanism shows that there needs to be a focus on social engineering penetration testing that only a hacker can provide. There is no way to automate art – the "White Hat" hacker wins again.

REFERENCES:

Ahn, W., Chung, M., Min, B. G., & Seo, J. (2015). Development of cyber-attack scenarios for nuclear power plants using scenario graphs. International Journal of Distributed Sensor Networks, 11(9), 836258.

Bishop, M., Coles-Kemp, L., Gollmann, D., Hunker, J., & Probst, C. W. (2010). 10341 Report--Insider Threats: Strategies for Prevention, Mitigation, and Response. In Dagstuhl Seminar Proceedings. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

Candell, R., Stouffer, K., & Anand, D. (2014, October). A cybersecurity testbed for industrial control systems. In Process Control and Safety Symposium, International Society of Automation, Houston, TX.

Gyunka, B. A., & Christiana, A. O. (2017). Analysis of Human Factors in Cyber Security: A Case Study of Anonymous Attack on Hbgary. Computing & Information Systems, 21(2), 10-18.

Midian, P. (2002). Perspectives on Penetration Testing—Black Box vs. White Box. Network Security, 2002(11), 10-12.

Mitnick, K. D., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. John Wiley & Sons.

Mitnick, K. (2011). Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. Hachette UK.

Pieters, W. (2011). Representing humans in system security models: An actor-network approach. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2(1), 75-92.

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical guide to information security testing and assessment. NIST Special Publication, 800(115), 2-25.

Tang, A. (2014). A guide to penetration testing. Network Security, 2014(8), 8-11.

Tischer, M et al., "Users Really Do Plug in USB Drives They Find," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2016, pp. 306-319.

Tomanek, M., & Klima, T. (2015). Penetration Testing in Agile Software Development Projects. arXiv preprint arXiv:1504.00942.

Watson, G., Mason, A., & Ackroyd, R. (2014). Social engineering penetration testing: executing social engineering pen tests, assessments and defense. Syngress.

Whitman, M. E. (2003). ENEMY AT THE GATE: THREATS TO INFORMATION SECURITY. Communications Of The ACM, 46(8), 91-95. doi:10.1145/859670.859675

Whitman, M. E., & Mattord, H. J. (2010, October). The enemy is still at the gates: Threats to information security revisited. In 2010 Information Security Curriculum Development Conference (pp. 95-96). ACM.

Wood, P. (2006). The hacker's top five routes into the network (and how to block them). Network security, 2006(2), 5-9.