POINTER: A GDPR-Compliant Framework for Human Pentesting (for SMEs)

J. Archibald and K. Renaud

School of Design & Informatics, Abertay University, Dundee, Scotland
e-mail:{j.archibald,k.renaud}@abertay.ac.uk

Abstract

Penetration tests have become a valuable tool in any organisation's arsenal, in terms of detecting vulnerabilities in their technical defences. Many organisations now also "penetration test" their employees, assessing their resilience and ability to repel human-targeted attacks. There are two problems with current frameworks: (1) few of these have been developed with SMEs in mind, and (2) many deploy spear phishing, thereby invading employee privacy, which could be illegal under the new European General Data Protection Regulation (GDPR) legislation. We therefore propose the **PoinTER** (**P**repare **TE**st **R**emediate) Human Pentesting Framework. We subjected this framework to expert review and present it to open a discourse on the issue of formulating a GDPR- compliant Privacy-Respecting Employee Pentest for SMEs.

Keywords

Penetration testing; Privacy Preservation; SME; GDPR

1 Introduction

Companies often employ security companies to test their systems' security: to detect vulnerabilities. This procedure is referred to as "*carrying out a penetration test*" (pentest), which aims to reveal vulnerabilities in the company's defences. The idea is that these can be addressed before malicious actors potentially find and exploit them. SMEs are in an unenviable position of being increasingly targeted by cyber criminals, and not having the financial resources to defend themselves as well as large companies can (Saleem *et al.*, 2017; Wlasuk, 2012). It has been estimated that as many as 60% of small businesses who experience an attack go out of business so this matter needs urgent attention.

Even if an SME *can* afford to have a penetration test carried out, there are two problems. The first is the nature of the penetration tests themselves, which are often technically-focused (Yeo, 2013; Tiller, 2004; Bacudio *et al.*, 2011). The second is that the pentest frameworks are generally constructed with larger companies in mind, especially when it comes to remediation, which is often unrealistic given SMEs' limited resources (Berger & Jones, 2016).

2 Human-Centred Penetration Testing

Most penetration tests, by focusing on technical vulnerabilities (Staiwan *et al*., 2017; Tang, 2014; Xynos *et al*., 2010), neglect the human's role in the security loop. To ensure that a full range of vulnerabilities are detected, a penetration tester should also test human resilience to attack. This is especially important because recent reports reveal that three quarters of organisations, across the board, experienced a phishing attack in 2017. (GOV.UK, 2018)**.** Few tests are specifically tailored to the SME context (Berger & Jones, 2016) and technical penetration tests cannot reliably identify human vulnerabilities.

Some researchers have proposed methodologies for human-focused pentesting, but many of these target employees with spear phishing attacks. This is problematical because the effective spear phish relies on the pen tester uncovering personal details and figuring out how to exploit their new knowledge of the employee's personal interests and concerns. This could be considered an unacceptable violation of their privacy, especially in the light of the new General Data Protection Regulation (GDPR) legislation (https://gdpr-info.eu/) (Kenner, 2017).

While hackers undeniably deploy spear phishing as an attack vector (TREND Micro, 2012), and many are specifically targeting SMEs (Pickard-Whitehead, 2017), it does not seem appropriate for the "good guys" to appropriate techniques used by the "bad guys". Pen testers aim to practice their skills ethically and defensively, as suggested by their title. In this respect, they are fundamentally different from the usual cyber attacker: their ethical perspectives are diametrically opposed. Hence, we need to consider developing a *privacy-respecting GDPR-compliant* human pentest framework to inform the pentesting industry at large.

We set out to develop this framework, which can be used by pentesters when probing and revealing the SME employee vulnerabilities. Before we discuss the framework, we first address the ethics of spear phishing, when carried out by pentesters.

3 Human Pen Testing: Privacy & GDPR

Social engineering attacks target employees, both digitally and otherwise. Social engineers use email, SMS, phone, removable media and in-person interaction to manipulate individuals to carry out actions the social engineer wants them to perform.

When carrying out a spear phishing attack, a hacker will research an employee's personal interests on social networking websites. The knowledge is used to construct an enticing phishing message redirecting the employee to a reputable looking website. Scattergun phishing attacks, on the other hand, send out generic messages to a wide range of targets and do not attempt to match messages to people's specific interests. Both of these can be used by pentesters, with the former having a much greater chance of success (Team Graphus, 2017).

When a pentester tests for resilience to spear phishing, he/she is essentially authorised to utilise the online footprint of key privileged employees in an organisation. A profile is constructed to tailor emails that are likely to engender trust via familiarity. If the targeted employee clicks on the embedded link, a number of different strategies can be deployed. Kumaraguru *et al*. (2009) suggests forwarding the person directly to a page that explains how to resist these kinds of attacks. They call this the "teachable moment". This approach has been adopted by some companies[1]. Others require the deceived employee to engage in an online training course[2] or report the employee to their line manager.

There is evidence that employees are angered by these kinds of approaches, considering them to breach the trust that ought to exist between employer and employee[3]. More importantly, it probably violates the new GDPR regulations, even if the personal information it uses is publicly available. The British Heart Foundation and RSPCA were fined recently for using publicly available information to target wealthy donors: they were using the information for a purpose the information's owner had not approved it for (Information Commissioner, 2016). GDPR explicitly forbids unauthorised use of personal data and pentesters might be sanctioned for engaging in such activities.

What about the pentester, on a personal level? If they have to carry out an intensive investigation into some person's life in order to carry out a spear phishing or social engineering attack, both the pentester and the employee are potentially harmed. The pentester cannot subsequently un-know everything they have discovered and could become deeply uncomfortable about having to invade another person's privacy in this way in order to carry out the pentest. The employee's privacy is certainly being sacrificed for the company's benefit. While employers can require particular standards of behaviour at work, they do not have the right to pry into their employees' personal lives (Pincus & Trotter,1995; Richman, 2000). Moreover, such activities violate one of the core tenets of ethical practice: respect (Frankena, 1986).

The argument *for* spear phishing employees, or exploiting them through other aspects of social engineering, is that this mirrors what hackers might do to compromise the organisation. It could also be argued that assessing the extent of publicly-available personal information online may assist the affected employee to strategically reduce or restrict the size of their online footprint. Yet there is an undeniable "creepiness"

[1] https://www.darkreading.com/risk/how-lockheed-martin-phishes-its-own/d/d-id/1139629; http://theinstitute.ieee.org/technology-topics/cybersecurity/company-tests-how-employees-handle- social-engineering-attacks

[2] http://www.govtech.com/security/Employee-Phishing-Expeditions-Among-States-Assessments- of-Cybersecurity-Awareness.html

[3] http://www.nj.com/healthfit/index.ssf/2016/06/in_security_test_hospital_phishes_its_own_employee.html

about an employer permitting this kind of investigation into their employees' personal lives (Rosenquist, 2015).

An open question is whether the new GDPR regulation permits this kind of action by employers. Spear phishing campaigns, in particular those conducted by pen testers, undeniably gather very personal data about employees that they have not provided for this purpose, which conflicts with the *raison d'être* of the new regulations.

However, the most compelling reason not to carry out spear phishing attacks on employees is revealed by recent research published by Caputo *et al.* (2014). They found no evidence that such efforts impacted subsequent link clicking behaviours, and therefore question the efficacy of the technique.

4 Developing a Privacy-Sensitive Employee Pen Test

Aim: Formulate a rigorous, comprehensive and dynamic pentesting process. This will be scientifically derived and refined rather than ad-hoc, the main feature of current testing regimens, as follows:

1. Carry out a literature review, investigating both research literature and publications from standards bodies and industry white papers. This will gauge the current "state of play" related to pentesting in the field.
2. (a) Construct an SME-specific pentesting framework that informs the investigation of employee-related vulnerabilities.
   (b) Suggest remediation actions that can be taken by organisations to address identified vulnerabilities.
3. Have the framework assessed by experts in the field, in order to refine and improve it.

4.1 Literature Review

The use of Social Engineering to exploit organisations has become more pervasive in recent times (Ashford, 2018; Costa, 2016; Weeks 2018; Smith, 2016). A human-centred penetration test can uncover vulnerabilities that make organisations open to social engineering attacks. Processes and frameworks that constitute human-centred penetration testing are discussed. We also consider whether these approaches are privacy sensitive and thus GDPR compliant.

The pretext to any penetration test is that it should be conducted in a legal and ethical manner. Prior to the test, consent must be given and signed off, a contract drawn up and appropriate people made aware that the test will take place (CSO, 2018). Any steps taken during the test must be lawful within the legal jurisdiction of the penetration test location (CSO, 2018; Ackroyd, 2014). In terms of ethical conduct, no one should come to any harm during a penetration test.

The Open Web Application Security Project (OWASP) is an open community which encourages organisations to create and work with trusted applications. OWASP

recommend a number of Penetration Testing Methodologies. (OWASP, 2016) Two of the recommended include a human centred element:

(1) Penetration Testing Execution Standard (PTES) which includes Pre-engagement Interactions, Intelligence Gathering, Threat Modelling, Vulnerability Analysis, Exploitation, Post Exploitation and Reporting (PTES, 2012a)
(2) Penetration Testing Framework (PTF) is technically oriented with tool recommendations but also lists human centred approaches such a Vulnerability Analysis and Physical Security.(OWASP, 2016)

Although both of the above consider human aspects of pentesting, neither consider the privacy of the employees. For example, PTES lists, as part of its Technical Guidelines, a range of social networking sites to use for gathering information, some of which could contain private and sensitive information, e.g. gays.com (PTES, 2012b)

The Council for Registered Ethical Security Testers (CREST) (CREST, 2017) is an Accreditation Body for the information security industry and provide guidance in running Penetration Testing programmes. They recommend the following as good practice advice:

(1) Open Source Security Testing Methodology Manual (OSSTMM) includes a chapter on Human Security Testing
(2) National Institute of Standards and Technology (NIST) Special Publication 800-115 (SP800-115), includes a section on Social Engineering
(3) Information Systems Security Assessment Framework (ISSAF) includes a chapter on Social Engineering

Similar to the OWASP recommendations, none of the above consider approaches to help maintain the privacy of employees involved in a penetration test. Although (NIST) (SP800-115) and OSSTMM do mention that effects of penetration testing on employees should be considered. By not respecting privacy rights, there is the possibility that a penetration test may violate GDPR regulations.

Ackroyd (2014) and Dimkov *et al., (*2010) addressed the issue of privacy and developed methodologies which attempted to make penetration testing easier on the employee. However their methodologies are oriented towards larger organisations and thus not appropriate for SMEs. In terms of the size of companies, none of the literature specifically considers a Human-centred approach to penetration testing for SMEs. However there is evidence that SMEs are indeed targeted by social engineering attacks (Smith, 2016). Thus, testing resilience to mitigate against these attacks would be beneficial, especially if privacy-respecting and GDPR compliant.

4.2 SME-Specific Human Pentesting Framework

We suggest a three-phase penetration testing framework to guide and inform ethical penetration testers carrying out human penetration tests: (1) Pentest Preparation, (2) Pentest execution, and (3) Remediation.

We asked five experienced penetration testers and security experts to comment on:|

(1) Whether the framework covers all the aspects of penetration testing.
(2) Whether it respects privacy.
(3) Whether it is feasible for SMEs to apply the suggested remediations.
(4) Whether they can suggest any refinements or improvements.

Based on their feedback, we refined and improved the framework, which we provide in the next Section.

5 Final Framework

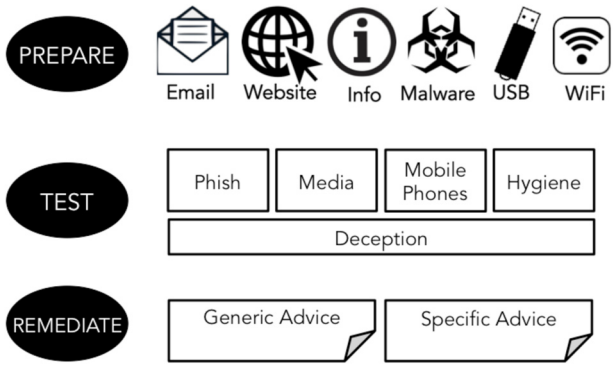

Figure 1: The **POINTER** Human Pentest Framework.
Pentester prepares materials, then tests human within workplace and offers remediation advice. No personal details will be recorded or included in reports.

Phase 1: Pentest preparation: (Ackroyd, 2014)

1) Speak to the CEO about setting up a "bait" website to be used in phishing pentesting. We will refer to this website as ***BAIT*** in the future discussion.
2) Tailor malware to be used in pentesting such that it reports only installations, but not the identity of the employee. We shall refer to this as ***TITBIT*** in the future discussion.
3) Set up an email address that looks similar to the CEO's: the ***DOPPELGANGER***.
4) Ask the CEO to give all his employees a confidential mobile phone number, to be used only in emergencies. This will entail loaning a mobile phone to the

CEO with a new SIM card in it (this can be reused). This number will be referred to as ***CEO-Mobile***.

5) Prepare **USB** sticks for distribution.
6) Set up a **rogue** WiFi.

Phase 2: Pentest execution: The pentest should cover the following areas (Kelm, 2014, Acquisti *et al*, 2017; Coventry *et al*., 2014; Yevseyeva *et al.,* 2014; Denno, 2016, Ackroyd, 2014):

1) **PHISH:**
   a) ***PHISH with LINK***: The ***DOPPELGANGER*** sends a Phish message with an embedded link that redirects to the BAIT website put up by the pentester which appears to offers some very useful functionality appropriate to that particular company (as agreed by the CEO of the company)
      i) See if you can get people to create an account (they might use the same password they have used on other sites). Keep a tally of these
      ii) Execute a drive-by attack which essentially reports to the pentester that the an employee visited the website.
   b) ***PHISH with Malware or HTML ATTACHMENT***: The ***DOPPELGANGER*** sends a Phish message that purports to come from the CEO, with an attached file (TITBIT) with embedded executable functionality. The TITBIT file executable should inform the pentester that it has been opened, but not who opened it.
   c) ***PHISH with PDF ATTACHMENT***: The ***DOPPELGANGER*** sends an email that purports to come from the CEO, with a PDF file attached. The file itself is fine, but there is an embedded link that is suspect. If clicked, it will redirect the employee to the BAIT.
   d) ***WHALING***: The ***DOPPELGANGER*** sends an email that purports to come from the CEO, which asks the person to download a particular file and attend to it urgently. The link is similar to those generally used within the company. This could be Dropbox or Google Docs, for example. If clicked, this will redirect the employee to the **BAIT** website, which records the visit.
2) **MEDIA Drop (deception)**: Drop USB sticks with a folder called SECRET-IMAGES. The folder is full of files with extensions like ".png", "pdf" or ".jpg" but one or two (with enticing names) are actually exe files which will inform the pentester that they have been opened.
3) **Deception:**
   a) ***In Person***: Elicit the assistance of a fellow pentester who is not known to the company. They should arrive at the company with some kind of story, in order to persuade someone to "help" them by printing a CV from a USB stick. If an employee can be persuaded to plug in the USB stick, an executable will inform the pentester.
   b) ***Telephone Call***: Call and tell an employee a story about a very urgent need to contact the CEO, and try to elicit **CEO-Mobile**.
4) **Good Hygiene**:

a) ***Workplace***: Walk around the office space at the end of the day and see whether any computers have been left unlocked, whether mobile media have been left lying around.
   i) If anything is found, secure and return to owner.
   ii) If a computer is left unlocked, make a note of what functionality an attacker could have gained access to.
   iii) Check for confidential material in dustbins
   iv) Passwords: Check for WiFi and/or personal passwords publicly displayed in offices or hidden under keyboards. Check for written records of passwords. Check under keyboards and around desks for hidden post-it notes with passwords.

b) ***Backups***: Find out how backups are secured. Check whether these are encrypted.

c) ***Awareness***: Plug an inactive keylogger into a machine's USB (at the front of the machine) and see whether anyone spots it.

5) **Mobile Phones**: If people are permitted to read their work email on their phones, or use the company WiFi, check that employees:
   a) control access to the phone with a PIN/Password or Fingerprint (not Pattern).
   b) understand the need to limit permissions given to Apps installed on the phones.
   c) are in the habit of updating phones and apps to the latest version.
   d) use the company VPN if applicable.
   e) connect to the **rogue** WiFi hotspot you set up.

Phase 3: Remediation: Here we suggest two kinds of remediation:

5.1 Generic Advice

1) Identify a few approved password managers for the employee to choose from. Strongly recommend usage and provide installation support.
2) Recommend an organisation-approved VPN with multiple licences so all employees can use it on their mobile phones.
3) Ensure that technical measures are the first defence. Only where technical measures cannot detect attacks should the company rely on the users to detect anomalies. Examples are: group policies that prevent external storage devices from being access from computers, password protected screen savers and only admins can run executable files.
4) Institute a training programme so that staff know about hovering over a link to check the actual destination of links, which they should examine for authenticity. They should have the freedom to report links they are unsure about to their security staff, without risk of censure.
5) Lay down a clear policy for what to do should someone click on a link, or open a suspicious attachment.
6) If employees are permitted to read their work emails from their phones, or use the company network, ensure that minimum security standards have been implemented on the phone before access is permitted. Ask for a copy of their BYOD policy.

5.2 Specific Advice

1) Depending on the outcome of the pentest, deliver specific advice related to Phish resilience.
2) The approach should be to find out how to make compliance as easy as possible for employees. Punishments, shaming and excessive imposition of rules to control behaviour are counter-productive and ought not to be seen as the solution to any security weaknesses.
3) Depending on the identified vulnerabilities, recommend specific training to be delivered to employees.

6 Conclusion & Future Work

In this paper we report on the development of a penetration test that seeks to test employee resilience. We argue that such frameworks ought to be sensitive to ethical

issues, GDPR regulation and privacy preservation. We argue that the privacy of employees should be respected and preserved. We asked five security experts to comment and refined the framework based on their feedback. We are planning to give this framework to some student penetration testers to use so that we can gather feedback about how viable, helpful and effective it is in practice.

7 References

Ashford, W. 2018. More than one in 10 employees fall for social engineering attacks, Available from: https://www.computerweekly.com/news/252438572/More-than-one-in-10- employees-fall-for-social-engineering-attacks (Accessed 16 May 2018)

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F., Sleeper, M. and Wang, Y. 2017. Nudges for privacy and security: Understanding and assisting users' choices online. ACM Computing Surveys (CSUR), 50(3), p.44.

Bacudio, A.G., Yuan, X., Chu, B.T.B. and Jones, M. 2011. An overview of penetration testing. International Journal of Network Security & Its Applications, 3(6), p.19.

Berger, H. and Jones, A. 2016, July. Cyber Security & Ethical Hacking For SMEs. In Proceedings of the 11th International Knowledge Management in Organizations Conference on the changing face of Knowledge Management Impacting Society (p. 12). ACM.

Caputo, D.D., Pfleeger, S.L., Freeman, J.D. and Johnson, M.E. 2014. Going spear phishing: Exploring embedded training and awareness. IEEE Security & Privacy, 12(1), pp.28-38.

Costa, C. 2016. Protect Yourself and Your Business from Social Engineering. Available from: https://www.sitepoint.com/protect-yourself-and-your-business-from-social-engineering/ (Accessed 16 May 2018)

Coventry, L., Briggs, P., Jeske, D and van Moorsel, A. 2014. Scene: A structured means for creating and evaluating behavioral nudges in a cyber security environment. In International Conference of Design, User Experience, and Usability. Springer, 229–239.

CREST. 2017. Penetration Testing - A Guide for Running an Effective Programme Available from: http://www.crest-approved.org/a-suppliers-guide-to-penetration-testing-services/index.html (Accessed 16 May 2018)

Denno, J. 2016. Attacking the Human - The Weakest Link in Cybersecurity. Masters Thesis. Utica College.

Evans, N.J. 2009. Information technology social engineering: an academic definition and study of social engineering-analyzing the human firewall. PhD Dissertation. Computer Engineering. Iowa State University.

Frankena, W.K. 1986. The ethics of respect for persons. Philosophical Topics, 14(2), pp.149-167. GOV.UK, 2018. Cyber Security Breaches Survey 2018, (Accessed 16 May 2018). Available from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018.

Information Commissioner. 2016. ICO investigation reveals how charities have been exploiting supporters, (Accessed 16 May 2018). Available from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/12/ico-investigation-reveals-how-charities-have-been-exploiting-supporters/

Kelm, D. 2014. FoSA - Framework for Social Engineering Auditing, Masters Dissertation. Technische Universität, Darmstadt.

Kenner, M. 2017. Video surveillance at work breached employee privacy, ECHR rules. https://www.peoplemanagement.co.uk/news/articles/video-surveillance-breached- privacy. Accessed July 2018.

Kumaraguru, P., Cranor, L.F. and Mather, L. 2009. Anti-phishing landing page: Turning a 404 into a teachable moment for end users. In Conference on Email and Anti-Spam (CEAS).

OWASP. 2016. Penetration Testing Methodologies, (Accessed 16 May 2018) Available from https://www.owasp.org/index.php/Penetration_testing_methodologies

Pickard-Whitehead, G. 2017 10 Phishing Examples in 2017 that Targeted Small Business. Aug 29. https://smallbiztrends.com/2017/08/phishing-examples-small-business.html (Accessed 16 May 2018)

Pincus, L.B. and Trotter, C. 1995. The disparity between public and private sector employee privacy protections: A call for legitimate privacy rights for private sector workers. American Business Law Journal, 33(1), pp.51-90.

PTES, 2012a. PTES Technical Guidelines, Available from http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines (Accessed 4 June 2018)

PTES, 2012b PTES Technical Guidelines, Social Networking Websites, (Accessed 16 May 2018)
http://www.penteststandard.org/index.php/PTES_Technical_Guidelines#Social_Networking_Websites (Accessed 4 June 2018)

Richman, A. 2000. Restoring the Balance: Employer Liability and Employee Privacy. Iowa Law Review, 86, p.1337.

Rosenquist, M. 2015. How Far Should a Company go to Test Employee's Resistance to Phishing. https://itpeernetwork.intel.com/how-far-should-a-company-go-to-test-employees-resistance-to-phishing/. August 13 (Accessed July 2018).

Saleem, J., Adebisi, B., Ande, R. and Hammoudeh, M. 2017, July. A state of the art survey-Impact of cyber attacks on SME's. In Proceedings of the International Conference on Future Networks and Distributed Systems (p. 52). ACM.

Smith, M. 2016. Social engineers reveal why the biggest threat to your business could be you. Aug 4. https://www.theguardian.com/small-business-network/2016/oct/04/social-engineers-reveal-biggest-threat-business (Accessed 16 May 2018)

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

Team Graphus. (2017) Verizon Says Phishing Still Drives 90% of Cybersecurity Breaches. 2017. https://www.graphus.ai/verizon-says-phishing-still-drives-90-cybersecurity-breaches/ (Accessed 16 May 2018)

Tiller, J.S. 2004. The ethical hack: a framework for business value penetration testing. CRC Press.

TREND Micro. 2012. Spear-Phishing Is the Favored Targeted Attack Bait. November 28. https://www.trendmicro.com/vinfo/au/security/news/cybercrime-and-digital-threats/spear-phishing-is-the-favored-targeted-attack-bait (Accessed 16 May 2018)

Wlasuk, A. 2012. Small Business and Law Firms-Protecting the Security Interests of Clients. Vermont Bar Journal, 38, p.32.

Weeks, R. 2018. Five common social engineering attacks and small businesses. Available from: http://smallbusiness.co.uk/five-common-social-engineering-attacks-cybersecurity-training-2542739 (Accessed 16 May 2018)

Xynos, K., Sutherland, I., Read, H., Everitt, E. and Blyth, A.J. 2010. Penetration testing and vulnerability assessments: A professional approach. Proceedings of the 1st International

Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 23rd August 2010

Yevseyeva, I., Morisset, J., Turland, Coventry, L., Groß, T., Laing, C., and van Moorsel, A. 2014. Consumerisation of IT: Mitigating risky user actions and improving productivity with nudging. Procedia Technology 16 (2014), 508–517.

Yeo, J. 2013. Using penetration testing to enhance your company's security. Computer Fraud & Security, 2013(4), pp.17-20.