Refining the POINTER "Human Firewall" Pentesting Framework

Abstract

Purpose

Penetration tests have become a valuable tool in the cyber security defence strategy, in terms of detecting vulnerabilities. Although penetration testing has traditionally focused on technical aspects, the field has started to realise the importance of the human in the organisation, and the need to ensure that humans are resistant to cyber-attacks. To achieve this, some organisations "pentest" their employees, testing their resilience and ability to detect and repel human-targeted attacks. In a previous paper we reported on PoinTER (Prepare TEst Remediate), a human pentesting framework, tailored to the needs of SMEs. In this paper, we propose improvements to refine our framework. The improvements are based on a derived set of ethical principles that have been subjected to ethical scrutiny.

Methodology

We conducted a systematic literature review of academic research, a review of actual hacker techniques, industry recommendations and official body advice related to social engineering techniques. To meet our requirements to have an ethical human pentesting framework, we compiled a list of ethical principles from the research literature which we used to filter out techniques deemed unethical.

Findings

Drawing on social engineering techniques from academic research, reported by the hacker community, industry recommendations and official body advice and subjecting each technique to ethical inspection, using a comprehensive list of ethical principles, we propose the refined GDPR compliant and privacy respecting PoinTER Framework. The list of ethical principles, we suggest, could also inform ethical technical pentests.

Originality

Previous work has considered penetration testing humans, but few have produced a comprehensive framework such as PoinTER. PoinTER has been rigorously derived from multiple sources and ethically scrutinised through inspection, using a comprehensive list of ethical principles derived from the research literature.

1. Introduction

The Federation of Small Businesses (FSB) reports that there were 5.6 million small businesses in the UK at the start of 2018, providing 60% of all private sector employment in the UK. The UK's National Cyber Security Centre (NCSC) (2017) published a cyber security guide for small businesses. They commence by saying that small businesses have a 1 in 2 chance of experiencing a cyber security breach, which could result in a loss of £1400. The incidence of breaches is confirmed by a report published by Kaspersky in 2017, which reported that almost half (42%) of the SMEs they surveyed had indeed experienced at least one data breach. In terms of consequences, The Information Security Breaches Survey 2014[1], commissioned by the Department for Business, Innovation and Skills (BIS) and carried out by PwC, reported that the worst SME-related breaches cost between £65,000 and £115,000, on average. Liwer (2018) reports that 60% of hacked small businesses do not recover and stop trading as a consequence of being attacked. The sheer scale of the problem could have a devastating effect on the UK economy and needs serious attention.

[1] https://www.gov.uk/government/news/cost-of-business-cyber-security-breaches-almost-double

Why are SMEs so vulnerable? Kaspersky (2017) reports that the majority of SMEs (72%) were sure they were reliably protected from cyber attacks. This mistaken sense of invulnerability suggests either that they do not understand how to detect vulnerabilities or that they are reluctant to search for vulnerabilities. Liwer (2018) suggests that this is due to the fact that they usually do not employ in-house IT staff to take care of security, nor are they able to train their staff as large organisations are able to do. It could also be that larger businesses are becoming harder to attack, leading cyber criminals to look for easier targets. SMEs are thus 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).

The National Cybersecurity Centre (NCSC) (2017) provides five distinct sets of advice to small businesses to help them to prevent such a breach from occurring. Even if SMEs *do* follow this advice, it is important to test the efficacy of the measures they are taking, especially in the light of the new European GDPR legislation, which can impose significant fines in the case of a data breach.

Employees are often considered both the greatest asset in an organisation, and the most vulnerable target of hackers (Olavsrud, 2014, p. 5). Burkhead (2014) says "*There are many different types of technology vulnerabilities and processes for attacking them with many different results; however, the one constant is the human aspect of information security*" (p.50). Humans trust other humans; that is the reality, and we cannot change human nature (Thornburgh, 2004; Abraham & Chengalur-Smith, 2010). Yet we can make people more aware of the nefarious techniques used by hackers deploying social engineering techniques.

SMEs can employ security companies to test their systems' security. In this way vulnerabilities can be detected by an impartial and objective party. Most important is the fact that this investigator is not malicious. 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. Many penetration tests are primarily focused on detecting technical vulnerabilities (Yeo, 2013; Tiller, 2004; Bacudio *et al.*, 2011; Cooper, 2017). Even the NCSC's guidance on penetration testing does not include any advice on how to pentest the human in the socio-technical system[2].

We commence our discussion with a brief review of social engineering, and of penetration testing's role in resisting such efforts. We then report on a systematic literature review of research into human-focused pentests, in order to compile a full list of tests that ought to be carried out. We also looked at what hackers themselves have to say about how they exploit humans, and then what cybersecurity industry reports say about how to defend against human-targeted hacks. Finally, we reviewed the advice that official bodies give with respect to making the human in the socio-technical system resilient to such attacks. Because our framework seeks to be ethical, we then proceeded to compile a comprehensive list of ethical principles from the research literature, which we used to filter out techniques that could be considered to be unethical.

In concluding, we propose a refinement of the GDPR compliant and privacy respecting PoinTER (Prepare TEst Report) Human Pentesting Framework (Archibald & Renaud, 2018). The techniques included in the refined framework have been rigorously derived and ethically scrutinised. The research methodology is depicted in Figure 1.

Figure 1: Depiction of Research Methodology
(*Ti* = Social Engineering Techniques, *Ei* = Ethical Principles)

[2] https://www.ncsc.gov.uk/guidance/penetration-testing

2. Social Engineering: Context

2.1 A Historical Perspective

Social engineering is an ancient technique. The difference now is that the social engineer can approach and exploit a victim remotely, without needing to be in the same time and place as the victim. Some examples of historical social engineering will illustrate the roots of modern social engineering. Consider the biblical story of Adam and Eve, who were told not to eat fruit from the tree of life. Yet the snake (the social engineer) enticed Eve to eat the fruit, and she took the bait. In Greek mythology, the leader of the Greek army tricked the Trojan army offering them a gift of a huge wooden horse better known as the Trojan Horse (Burton, 1979). The Trojans accepted the gift of the horse, dragged it into their enclosure, and thereby allowed the attackers in, in much the same way as Phish recipients unwittingly permit Phishers to access their systems. In the 1960's, Frank Abagnale successfully impersonated a commercial pilot, a doctor, a lawyer, and a teacher (Abagnale & Redding, 2003) and Kevin Mitnick (Mitnick and Simon, 2011) was also able to impersonate someone in authority to gain access to company premises.

2.2 Exploiting Human Nature

As the social engineers in history found, they could rely on people's tendency to be helpful and empathetic; exploiting the best of human nature to compromise security (Chabrow, 2008). Hinson (2008) explains that social engineers exploit the human tendency to trust, helpfulness, respect for authority, unawareness, and carelessness. These are also mentioned by Luo *et al.* (2011) and Applegate (2009). Hasan *et al.* (2010) refers to the ordinary employee's inability to second guess people's actual motives, which allows social engineering attacks to succeed. One could refer to this as gullibility, which occurs due to a lack of awareness of social engineer techniques. Thornburgh (2005) also refers to this aspect, and adds greed, fear and empathy as human tendencies that social engineers exploit. Fear and empathy are also mentioned by Rader *et al.* (2013). Mouton *et al.* (2016) add the establishing of rapport between social engineer and target victim. Chantler & Broadhurst (2006) mention triggering a strong emotion, helpfulness, and respect for authority, as well as overloading the senses of the victim so that he or she is more likely to act without due consideration . Krombholz *et al.* (2014) adds curiosity to this list, which is also confirmed by Rader *et al.* (2013).

Wright *et al.* (2014) explore the use of *persuasion* in social engineering attacks. Greavu-Şerban & Şerban (2014) refer to specific persuasion techniques: simplicity,self- interest, incongruity, confidence, trust and empathy. Cialdini (2001), a persuasion expert, mentions core principles of persuasion: reciprocity, social proof, sympathy, authority, consistency, and rarity. Chantler and Broadhurst (2006) also mention reciprocation in the establishing of a relationship between deceiver and victim.

Oliviera *et al.* (2017) mention the way social engineers exploit personal vulnerabilities, which they discover by doing research into the victim's personal interests, and thereby enticing them to click on a link.

Actual Attacks: Nelms *et al.* (2016) reviewed hundreds of social engineering attacks and provide a detailed analysis of the techniques used by social engineers based on a study of 2004 attacks. They report that the top three techniques used by social engineers are *alarming* (21.6%), *enticing* (48.5%) and *invoking compliance* (19.16%). Tetri and Vuorinen (2013) also mention *manipulation* and *flirting*.

All of these exploits would not work on a computer, because computers do not have humanity. The social engineer exploits the best of human nature to achieve their nefarious aims. This makes such attacks particularly challenging to train people to resist. The next sections will consult a number of sources to compile a list of techniques used by social engineers to exploit these aspects of human nature.

2.3 Penetration Testing

Pentest plans are usually formulated with larger companies in mind, especially when it comes to proposed remediations, which is often infeasible for SMEs to apply (Berger & Jones, 2016). The NCSC (2018) rates

hackers in terms of sophistication: (1) *None* ('Can carry out random acts of disruption or destruction by running tools they do not understand'), all the way through to *Minimal*, *Intermediate*, *Advanced*, *Expert*, and *Innovator*, to *Strategic* ('State actors who create vulnerabilities through an active program to influence commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest'). They recommend that, when looking at the cyber security of a company, to be specific about what security actually means. So, for example, for an SME, it might mean: "*Is it secure against attacks requiring an Intermediate level of capability?*".

Another aim could be to improve employee resilience, as opposed merely maximising resistance. Resistance is about avoiding adverse events (Arenaza-Urquijo and Vemuri, 2018). Resistance is only feasible when it is actually possible to avoid the risk being resisted. When 100% avoidance via resistance is impossible, we have to build resilience into the system too. Resilience is about learning to cope with the reality of a situation. It refers to a community's ability to recover to pre-event levels of functioning after an adverse event (Gardi *et al.*, 2009). There is a need to balance resistance and resilience efforts (Paz *et al.*, 2018). PWC says: "*achieving greater cyber resilience as a society and within organisations will require a more concerted effort to uncover and manage new risks inherent in emerging technologies*" (Castelli *et al.*, 2018)[p.10].

3. Systematic Literature Review

3.1 The Review

We conducted a rigorous literature search investigating the issue of pentesting employees within organisations. We searched through a number of databases from the year 2010 onwards, as detailed in Table 1. We concluded by checking Google Scholar for missing papers. We filtered out publications that were not written in English and excluded patents.

We used Google Scholar citation index service to perform a forward search. The backward search was conducted manually.

We used the following keywords for our search:

- human/employee/user pentest/"penetration test" ((human or employee or user) and (pentest or "penetration test"))
- "hacking the human"
- human/employee/user pentest/"penetration test"
- social engineering test employee/user (+ pentest/"penetration test")

We conducted a full-text search. The databases were searched to identify publications that contained at least one of the above combinations. We then applied the defined inclusion and exclusion criteria. Following this process, only 40 publications remained. Table 1 shows the number of publications for each database search; how many were excluded and how many were retained for analysis.

Table 1 shows the number of publications for each database search, how many were excluded and how many remained for analysis.

Source	***# Returned***	***# Eliminated***	***# Retained***
Theses: ProQUEST, Ethos, DART, PQDT, Ebsco	48	23	25
SCOPUS	1	1	0
ACM Digital Library	1	1	0
IEEE Xplore	3	2	1

Springer	1	1	0
JSTOR	2	0	0
ERIC	0	0	0
http://worldcat.org	3	3	0
Google Scholar	25	11	14

Table 1: Systematic Literature Search for Relevant Publications

Table 2 now presents the outcome of our analysis of the 40 publications related to human-related hacking. The papers' reported techniques fell naturally into six categories.

Issue Addressed	**Aspects Studied**
Awareness	• Awareness & Training (Smith and Shorter, 2010; Chaudhury, 2016; Chuenchuji, 2016; Long, 2013; Tarallo, 2015; Snyder, 2015; Von Solms & Warren, 2011; Hadnagy, 2010; Spinapolice, 2011; Abraham & Chengalur-Smith, 2010; Schaeken, 2018; Tikkanen, 2017; Toussaint, 2015; Walker, 2016; Labossiere, 2015; Laribee, 2006; Beckers *et al.*, 2016; Schaeken, 2018; Walker, 2016; Halevi *et al.*, 2015) • Vaccinating via building Competence (Jansson, 2011) • Withstanding Deception Techniques: Having a plan, training people in implementing the plan, and incorporating the human elements of security into information security incident response (Burkhead, 2014).
Phishing Training	• Ethical experiments to mimic Phishing Attacks using opt out and debrief (Resnik and Finn, 2018) • Anti-phishing Framework (Frauenstein, 2013) • Trust focused education framework (AL-Hamar, 2010) • Security Primer for Senior Executives (Toussaint, 2015)
Measuring resilience to social engineering	• A COSO-focused Social Engineering Threat/Risk Assessment (Kiama, 2016) • Combining measuring exercises and penetration testing with training. (Nohlberg, 2008) • Conduct extensive security audits (Snyder, 2015) • Phishing IQ Test, Comics, Games (Chaudhury, 2016) • Leadership, Knowledge Sharing, Measurement Actual Behaviours (Flores, 2016; Okoye, 2017) • Vulnerability Assessments (Tarallo, 2015)
Counter measures	• Technical Detection (Edwards *et al.*, 2013; Chuenchujit, 2016) • Law and Regulation at global level, (Bendovschi, 2015), (DOGANA, 2016) • Strengthening Policies (Snyder, 2015; Okoye, 2017; Spinapolice, 2011; Tarallo, 2015) • Establish culture of security and accountability (Adewole 2015; Spinapolice, 2011)
Physical Access or Scouting	Develop scripts (Snyder, 2015; Hadnagy, 2010)
Social Media (enabling Scouting)	• Awareness of risks (Snyder, 2015) • Tailored training (Schaeken, 2018) • Age-related Targeted Training (Slonka, 2014)

Table 2: Categorising Reviewed Research Publications

3.2 Analysis

Few of the papers we review go into much detail about exactly how to "Penetration Test" the organisation's humans. Some do provide guidance that is helpful in informing the refinement of our PoinTER framework.

Hadnagy (2010) names key social engineering techniques (*Ti*) that an audit should address, as do others. Here is a superset of the techniques they mention:

- ***T1:*** *Phish employees*: (Bowen *et al.*, 2012). This is Nelm *et al* (2016)'s "enticing"; Abraham & Chengalur-Smith, 2010's greed/curiosity. This tests whether employees will click on links in emails or open attachments (simulated Phishing attack).
- ***T2:*** *Cloning Websites:* Determine whether an employee can be enticed to visit a website and provide their credentials to the site
- ***T3:*** *Ask for Information*:
    - Find out how much information can be obtained via the phone or in-person (Pretexting In-Person Attacks) (Cialdini, 2001's persuasion via authority, liking and consensus; Evans, 2009)
- ***T4:*** *Hygiene:* Assess physical security (Baiting, Piggybacking) (Lively 2003's Helpfulness attack vector)
- ***T5:*** *Media Drop*: See whether employees will plug a USB into their work computer (Nelm *et al* (2016)'s "enticing" and Abraham and Chengalur-Smith, 2010's curiosity)

4. How Hackers Exploit Humans

4.1 Exploitation

Dicosmo (2018) calls hackers "con artists", which means that they have a knowledge of human nature, and of how to exploit it. The techniques mentioned by Hadnagy (2010) exploit such human propensities. Mitnick, a well-known hacker who was arrested and served time for social engineering activities, said "*The key to social engineering is influencing a person to do something that allows the hacker to gain access to information or your network*." (Mitnick and Simon, 2011).

Given that Phishing is the most common method of social engineering[3], hackers are increasingly being brought to book for carrying out Phishing campaigns. Two recent examples are Eric Donys Simeu (Dark Reading, 2017) and Ryan Collins (Robertson, 2016). A number of famous attacks have been achieved by means of Phishing attacks:

- 2011: *RSA SecurID*. Attackers sent RSA employees an email with an Excel attachment titled 2011 Recruitment Plan. They opened it—and a zero-day Flash exploit installed itself onto their systems (Zetter, 2011)
- 2013: *Yahoo Customer Account Compromise*: A semi-privileged engineer at Yahoo fell for a spear phishing email. The hackers compromised more than 3 billion accounts (Larson, 2017).
- 2013: *Associated Press Twitter*: The attack began as a spear phishing email to Associated Press employees that appeared to come from other employees of the Associated Press. It came from the Syrian Electronic Army. The email included a link to a phishing site where the employees entered login information for the Associated Press Twitter account. The Syrian Electronic Army posted a tweet that the White House had been bombed and that President Obama had been injured. The DOW dropped 150 points—about $136 billion—before rebounding (Fisher, 2013).
- 2014: *Sony Pictures*: A phishing attack gave hackers access to Sony's systems. They lost a number of unreleased films and many personal emails (Alvarez, 2014)

[3] https://gdpr.report/news/2018/03/20/cyber-threatscape-top-10-phishing-emails-deemed-number-one-threat-by-uk-businesses/

- 2015: *Ubiquiti Networks Scam*: The accounting department received an email seeming to come from the company's Hong Kong subsidiary. It contained instructions changing payment account details, which the accounting department followed (Eng, 2015).

How else do hackers exploit people? Way back in 1981 a hacker called Captain Zap hacked into AT&T's computers. In an interview he said: "*The reality is that the likes of Microsoft and Oracle, the others who control the technologies that are now so fully entrenched in our so-called information society are still causing the failure of the security of millions due to their greed and inability to allow others to see the magic behind the scenes".* He explains: "*An authoritarian voice with the right combination of buzz words and a bit of humor will get you past anyone on the phone.*" In 2007, Carlos Héctor Flomenbaum gained employees' confidence at the ABM AMRO bank in Belgium over a year long period. He then stole 28 million dollars in diamonds simply by being charming and friendly to staff, leading them to give him access to secure boxes (Castle, 2007). In 2008, US Presidential candidate Sarah Palin's email account was accessed by a hacker called David Kernell, who used publicly available information about her to guess the answers to her security questions (WIRED, 2008).

These kinds of attacks might seem ancient history a decade later, but recent hacker arrests show that these techniques still work (Brewster, 2018). It does not seem to require much expertise to deploy social engineering techniques. In 2018, a British teenager, Kane Gamble, was sentenced to two years for impersonating the head of the CIA, and conning call centres into divulging confidential information (BBC, 2018). Justin Liverman (Thomson, 2017) was sentenced to 60 months for his part in attempting to hack US government websites. Liverman hired a phone spamming service to harass Deputy Director Giuliano, attempting to elicit fear and disruption, as part of a long-term social engineering drive. Another hacker, George Garofano, posed as a member of Apple's online security team and sent emails to the victims asking for their usernames and passwords (Grinberg & Chavez, 2018). Garofano stole personal photos, and was sentenced to 8 months in prison in May, 2018.

Curran (2018) spent three weeks reading a Russian hacker platform on the dark web. He reported that the hacking community actively supports each other, sharing exploits, even posting videos to make it easier for others to use the exploits. He discovered detailed instructions for social engineering: "*Social engineering, in terms of hacking, is when you use some clever psychology to make a member of a company trust you and bypass security protocol. A common one is to ring the customer support of a company, and mask your number to mimic that of an internal phone number. You then play the fool and say you can't access a website where you normally could have, and that it's important to access it for an angry client. You then give the customer support agent a link to the website. The catch, is that you have made a fake website which has a Trojan ready to be deposited on to the agent's computer. The hacker then has access to the company's internal network.*" This confirms the growing popularity of social engineering attacks.

4.2 Summary

The consolidated techniques suggested by this hacker review are (continuing numbering from the previous list):

T6: *Spear Phishing without permission:* exploiting vulnerabilities as explained by (Oliviera *et al.*,2017)
T7: *Guessing Passwords:* exploiting well-known human tendencies to choose passwords related to their personal lives (Stobert and Biddle, 2014).
T8: *In Person Impersonation:* as mentioned by Hinson (2008) and Chantler and Broadhurst (2006).
T9: *Vishing*: usually exploiting gullibility and respect for authority or even fear (Yeboah-Boateng & Amanor, 2014).

5. What does the Cybersecurity Industry Advise?

It is instructive to consider what cybersecurity professionals and companies have to say about hacking humans. Rayome (2018) says Social Engineering was the second most popular method used by cyber criminals in 2018 (25%). Goldschmidt (2018) says that social engineering is the new norm in hacking. The techniques he reports hackers using are (1) Phishing, (2) impersonating a legitimate visitor, (3) tailgating, (4) reading RFIDs of access cards by standing close to an employee, (5) posing as a contractor. He considers raising awareness to be the key to building employee resilience. He also suggests sending out fake Phish messages to measure resilience. He recommends improving physical access systems to make it harder for hackers to gain physical access. Finally, he recommends including employees in company defence protocols i.e. ensuring that they are considered part of the company's cybersecurity defensive perimeter.

Mitnick (2018) mentions a number of hacker tricks: (1) targeting non-IT staff with Phishes, (2) cloning well--known websites and enticing staff into visiting these, (3) creating a WiFi hotspot and enticing people to connect to these. He recommends awareness-raising sessions and regular penetration testing as ameliorations.

Tulloch (2018) interviewed Sergii Nesterenko, a cybersecurity consultant and penetration tester, about cyber security. He mentions the following tests: (1) Phishing messages that trigger an emotion such as fear or greed, or (2) impersonating a trusted entity, He argues for raising awareness and creating competency.

Lanier (2018) cites a number of techniques used by social engineers: (1) fake website, (2) impersonating IT helpdesk staff, (3) ROSE (Remote Online Social Engineering). This technique plays the long game, and is sometimes called catfishing (Jeske and Van Schaik, 2017). The hacker builds rapport with "marks" within an organisation. The aim is to elicit sensitive information, gather material for extortion, and persuade employees to take actions leading to compromises.

Cameron (2018) reports on a talk by Gizmodo, which mentioned techniques used by penetration testers: (1) cloning security badges, (2) wiretapping, (3) using a maid's sympathy to gain access, (4) pizza delivery, (5) scan RFID access control cards, (6) simply asking for information.

The Social Engineering Framework (Security by Education, undated) mentions testing using the following techniques: (1) Phishing, (2) Vishing, (3) Impersonation and (4) SMiShing.

The techniques that emerge from this review include:

T1, T2, T3, T9 *confirmed*
T10: *Enticing people to use a rogue WiFi*: exploits human desire for convenience (Mitnick, 2018)
T11: *SMiShing:* exploits some of the same human vulnerabilities mentioned in the previous section (Yeboah-Boateng & Amanor, 2014).

6. What Advice do Official Bodies Offer?

A number of official bodies issue SME-specific cyber advice, related to social engineering attacks, which direct us towards techniques we could use in our framework:

	T1: *Phishing*	***T2:*** *Cloning Legitimate websites*	***T5:*** *Media Drop*	***T8:*** *In-Person Attacks*	***T12:*** *Physical Security*
NCSC (2017)	•		•		
Get Safe Online[4]	•				

[4] https://www.getsafeonline.org/business-blog/five-cyber-security-tips-that-could-save-your-small-business/

London Digital Security Centre[5]	•		•		
Federation of Small Businesses(FSB)[6]	•		•	•	
Federal Trade Commission[7]	•				•
Federal Communications Commission (FCC)[8]	•		•	•	•
NIST[9]	•	•	•		•

Table 3: Advice from Official Bodies

The review summarised in Table 3 confirms ***T1, T2, T5, T8***, and introduces **T12**: Physical Security.

Having compiled a comprehensive list of social engineering techniques (*T1-T12*), we now consider the ethical considerations that should constrain the techniques an ethical pentester deploys.

7. Ethical Principles and Scrutiny

7.1 The Principles

When considering the ethics of hacking humans the literature suggest a number of principles that should be followed or avoided. Table 4 depicts these principles in relation to employees, the pentest authoriser and the pentester with their interdependence depicted in Figure 2.

		Hadnagy (2010)	Kennedy *et al.* (2011)	Pierce *et al.* (2006)	Finn (1995)	Resnik & Finn (2018)	Dimkov *et al.* (2010)	Allsop (2010)	Tiller (2004)	Failly *et al.* (2016)	Archibald & Renaud (2018)
Employees	E1: Attack an employee's family or friends	✕							✕		
	E2: Embarrass or blackmail an employee	✕					✕	✕	✕		✕
	E3: Target employee without permission		✕		✕	✕	✕				✕
	E4: Use Deception when it is avoidable			✕	✕		✕	✕			✕
	E5: Permit opt out					✓					
Pentest **Authoriser**	E6: Serve and Protect			✓						✓	
	E7: Avoid Conflicts of Interest			✓					✓		
	E8: Avoid False Positives and False Negatives			✓							
	E9: Carry out tests that deliver value				✓			✓			
	E10: Debrief post-test				✓		✓				
	E11: Minimise Risk				✓			✓		✓	

[5] https://londondsc.co.uk/essential-advice-for-small-business-cyber-security/
[6] https://www.fsb.org.uk/resources/top-five-cyber-security-tips-for-small-businesses
[7] https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
[8] https://www.fcc.gov/general/cybersecurity-small-business
[9] http://csrc.nist.gov/groups/SMA/sbc/documents/sbc_workshop_presentation_2015_ver1.pdf

		Hadnagy (2010)	Kennedy *et al.* (2011)	Pierce *et al.* (2006)	Finn (1995)	Resnik & Finn (2018)	Dimkov *et al.* (2010)	Allsop (2010)	Tiller (2004)	Failly *et al.* (2016)	Archibald & Renaud (2018)
Pentester	E12: Keep it legal	✓						✓	✓		✓
	E13: Consider consequences of actions to employee, business owners, clients		✓						✓		✓
	E14: Be malicious or stupid		✕					✕	✕		
	E15: Uphold the Security Profession			✓					✓	✓	✓
	E16: Do not cause productivity loss						✓				
	E17: Keep it Confidential and Honest								✓		

Table 4: Ethical Principles of Penetration Testing (✕ = Avoid; ✓ = Do This)

Figure 2. Ethical Pentesting Principles *E1-E17*

7.2 Ethical Scrutiny of Social Engineering Techniques

We now subject our list of social engineering techniques (*T1-T12*) to ethical scrutiny, using the ethical principles (*E1-E17*) in order to consider whether they are indeed ethical or not.

7.2.1 Scattergun Phishing

Many organisations phish their own employees, in order to test their ability to spot these emails. Indeed, a number of companies offer this as a service[10]. Yet Murdoch and Sasse (2017) argue that these campaigns are not only ineffective but actually damaging to organisations. At one organisation, an internal Phish simulation generated severe internal trust problems. That being so, should a human pentesting framework include a Phish simulation? If we decide not to include it, we do not test resilience for the method most likely to be used by social engineers. On the other hand, Caputo *et al.* (2014) found that these campaigns do not reduce the percentages of people falling for Phishing messages. Moreover, even experts fall for a well targeted Phish, despite their knowledge and experience[11]. Is it realistic to expect a one-off intervention, in the form of a simulated Phish, to improve security in the long term?

If the organisation *does* want to include a Phish simulation, is there a way of simulating a Phish campaign while minimising the negative effects reported by Murdoch and Sasse and respecting ethical principles E2-E5 in Table 4?

- In the *first* place, the Phish email should not look too much like a valid email sent from someone within the company. This kind of email may look too much like entrapment, and also, by using the name of an employee, the campaign might unwittingly cast mud in their direction and this mud might cling. The deception that is used should be mediated according to principle E4.
- *Secondly*, the Phish should not be targeted at the specific employee, i.e. not use data gathered about the employee to explicitly target the employee's weaknesses. This aligns with E3.
- In the *third* place, we need to think very carefully about what happens if people click. The PoinTER framework already does not identify those who fall for the Phish. If this were done, companies would probably want to use this information to either send people for more training, or to punish them in some way. This would conflict with principle E2.

[10] https://resources.infosecinstitute.com/top-9-free-phishing-simulators/#gref
[11] https://www.ncsc.gov.uk/blog-post/serious-side-pranking

7.2.2 Spear Phishing

Our review shows that hackers do indeed deploy spear phishing as an attack vector (TREND Micro, 2012), and many are specifically targeting SMEs (Pickard-Whitehead, 2017). Yet it does not seem appropriate for the "good guys" to appropriate techniques used by the "bad guys". Pentesters aim to practice their skills ethically and defensively, as encompassed in their title. In this respect, they are fundamentally different from the usual cyber attacker: their ethical perspectives are diametrically opposed. Hence, we consider the development of a privacy-respecting GDPR-compliant human pentest framework to be desirable and beneficial to the pentesting industry at large. Gathering personal information from the employee's social networking sites, we believe, has become illegal due to the GDPR legislation coming into force. SMiShing is dubiously legal too, since it uses personal mobile numbers for purposes not specifically approved by their owners.

We therefore add spear phishing *without permission* to the list of forbidden activities because it violates ethical principles E2-E5 in Table 4. Principle E1 might also be violated if the message appears to come from family or friends.

In some circumstances, executives of an organisation specifically want a pentester to check what information can be discovered about them online, so that they can act to reduce their exposure and the vulnerability this constitutes to the organisation. We could include this as a special extra activity in our pentest, on request, and require those being spear phished to have specifically granted signed permission to authorise the scouting activity that precedes this kind of campaign, respecting ethical principles *E2-E5*, and *E13-E15* in Table 4. It will be up to the individual pentester to decide whether to offer this test or not.

7.2.3 Ambiguous Legality

Some vulnerabilities mentioned by hackers and industry seem to be problematical, given the ethical hacker's desire to stay within the bounds of the law (Principle E17 in Table 3). For example, Goldschmidt (2018) talks about RFID spying. This could very well be considered to be a criminal act, and we cannot therefore include it in our framework. Trying to gain access to the site, in order to test perimeter controls, on the other hand, is legal as long as the pentest Authoriser has provided the ethical hacker with signer authorisation which he/she can produce if challenged by security staff. One of the most popular techniques used by hackers is *password guessing*, but this is ethically unsound and potentially criminal (E12), so we cannot include this activity on our pentest.

Another technique that seems to stray into the wrong side of the law is ROSE, as mentioned by Lanier (2018). This requires the hacker to exploit an employee's personal information in order to socially engineer them. Unless the employer has signed permission from the employee to use their personal information in this way, this kind of action could be considered unethical. Finally, any activity that could potentially compromise the privacy of staff should be avoided by ethical hackers, so as to ensure that GDPR regulation is not breached. That being so, wiretapping (Cameron, 2018) should probably be avoided (E12).

Finally, since our framework seeks to respect privacy, we will not be including any SMSishing simulations, because that would require us to use personal mobile numbers for pentesting purposes, which could be considered a GDPR violation (Principles E2-E5 in Table 4). Reading people's card RFIDs is also illegal, especially if the hacker unwittingly gains access to credit or debit card details (E12). Based on the ethical review, we retain the following techniques for the PoinTER framework.

Figure 3: Final List of Categories (mapped to Techniques)
(*Ti* = Social Engineering Techniques, *Ei* = Ethical Principles)

8. POINTER Human Pentesting Framework

8.1 The Framework

Phase 1: Pentest preparation:

Part 1 - Pentester visits Authoriser away from office to ask:

1) What information is valuable to the SME? (Palmer, 2001)
2) Agree the duration of the test (Allsop, 2010).
3) Agree on success/failure metrics (Allsop, 2010).
4) Get sign off from the Authoriser to carry out the human penetration test (Klevinsky *et al.*, 2002).
    a) If an accomplice will be helping the pentester to make phone calls or try to breach the physical perimeter, obtain a signed authorisation document for that person to carry with them in case they are challenged (Klevinsky *et al.*, 2002).
    b) Discuss options for the Scenario accomplice could use for phone call or breaching the physical perimeter
5) The SME should set up an email address such as: **report-phishing@sme.com** on the company domain, which can be used by employees to report a suspected phishing email, or if they realise they have been deceived.

6) To inform the pentest:
    a) Are employees allowed to connect to the company WiFi from their Smartphones?
    b) Go through the different meta categories and discuss each with the Authoriser, and get sign off for each.

7) Week before pentester visits:
    a) Authoriser should tell staff that an ethical hacker will be visiting to test the company's cyber security. No mention should be made of the fact that this is actually a human pentest.
    b) SME owner should give staff his new confidential mobile number, which is only for their use, but not to be given to anyone else. The ethical hacker loans him/her a mobile phone with this number so that calls to this number can be monitored.
8) Agree on schedule for reporting outcome (Allsop, 2010).

Part 2 - Pentester prepares Technical Components

A TITBIT - Malware to be used in pentesting that only reports installations but no other information

If Employee Phish is included in pentest:

BAIT - Website that employee will be redirected to if they click on links.

- Ensure that Google does not index the page
- Install Google Analytics to count hits.

DOPPELGANGER - Email address that looks similar to the SME owner's

Phish email texts - Depending on sign off from the Authoriser, four different messages might be needed. These might depend on the time of year (e.g. New Year sales), recent news reports (drone problems at Gatwick), a freebie (any desirable item), or a whaling message from the SME owner instructing the employee to respond with information.

If Media drop is included:

USB Sticks - Prepare USB sticks with TITBIT with an enticing file name.

Use a label that is likely to entice people to open the file on the stick. Use an old-looking stick, that looks as if it has been lost.

If Hygiene is included:

Rogue WiFi: Set up rogue WiFi with name that is similar to the SME's WiFi connection

If Deception is included

Scenario – Develop Scenario based on discussion for phone call and physical breach

For every visit:

Audit Trail: Set up a logbook, similar to the one shown in Appendix A, to ensure that all relevant actions are logged, both those of the ethical hacker, the accomplice and the employees. An audit trail is essential, especially to separate the actions of the pentester from a hacker should the organisation be hacked during a penetration test (Whitaker & Newman, 2005).

Phase 2: Pentest execution: The pentest should cover the areas mentioned in Table 4:

Depending on which of these Phishes is explicitly authorised:

- **PHISH with LINK :** (Nelm et al (2016)'s *enticing*) The DOPPELGANGER sends a Phish message with an embedded link that redirects to the BAIT website
- **PHISH with Malware** (Nelm et al (2016)'s *compliance*): The DOPPELGANGER sends a Phish message that purports to come from the SME owner, with an attached file (TITBIT) with embedded executable functionality. The TITBIT file should inform the pentester that it has been opened, but not who opened it
- **PHISH with PDF ATTACHMENT:** (Nelm et al (2016)'s *enticing*) The DOPPELGANGER sends an email that purports to come from the SME owner, 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
- **WHALING**: (Nelm et al (2016)'s *compliance* and *alarming*) The DOPPELGANGER sends an email that purports to come from the SME owner, 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.

If Media Drop is authorised

- **MEDIA Drop (*enticing*)**: 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.
- **MEDIA Plugged in (*deception*)**: Plug an inactive keylogger into a machine's USB (at the front of the machine) and see whether anyone spots it.

If Deception is authorised:

- **In Person**: Elicit the assistance of an Accomplice (Fellow pentester) who is not known to the company. They should arrive at the company with story (agreed Scenario), 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, and open a file, an executable will inform the pentester.
- **Vishing**: (Nelm et al (2016)'s alarming) Call and tell an employee a story (agreed Scenario) about a very urgent need to contact the SME owner, and try to elicit Confidential-Mobile.

If Hygiene test is authorised:

- 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.
- Check for information that could be used to aid an exploit:
  1) Displayed or written notes of passwords
  2) Confidential information left on desks

- *Mobile Phones:* Check that the employee ensures that access to the phone is mediated by means of a PIN/Password or Fingerprint (not Pattern).

Rogue WiFi: Check how many people connect to this

Phase 3: Report

Jenny Radcliffe, called "*The People's Hacker*" (O'Hora, 2018), talks about how friendliness and helpfulness can be exploited by social engineers. She recommends awareness drives and warns against blaming people who fall for social engineering attacks. She recommends engendering discussions about social engineering within the organisation. Hence our ethical framework will not identify employees who have been deceived or fallen for a Phish, or engaged in any ill-advised insecure behaviours, aligning with principle E2 in Table 3.

Kennedy et al (2011) consider the report to be the most important part of the pentest. They recommend three sections: (1) executive summary, (2) executive presentation and (3) findings. We add another section: (4) Best Practice Advice. Also, because this is a human pentest, we recommend that the one-page summary be disseminated to all employees to raise awareness and reassure staff that they were not identified in the report. An executive summary template is suggested in Appendix B. Below is our suggested report template.

8.2 Human Pentest Report Template

Title: Human Penetration Test for Company [SME]
Company Location: [address]
Date: [dd/mm/yy]
Penetration Tester: [Name]

1. Executive Summary
Broad brush report - answer the basic questions:

(1) what the vulnerabilities are (refer to findings section),
(2) how serious the vulnerability is (link to prevalence e.g. Nelms et *al*., 2016) and
(3) how to fix it (direct links to best practice advice).

2. Section Title
Details of Authorised Tests Carried out
Details of Tests carried out from Table 3: (1) Phish, (2) Media, (3) Deception, (4) Hygiene, (5) Mobile. Provide the texts of the Phish messages if these tests were carried out. Provide full details of the deception techniques used, and exactly when (times and dates) hygiene tests were performed.

3. Findings
Report on findings for each of the authorised tests (aggregated with no identifying information)

4. Best Practice Advice
As detailed below, with links to *Findings* subsections where appropriate

1) **PHISH**:
   a) *Don't train staff to fall for Phish:* The most pernicious mechanism used to hack humans is the Phish. Organisations sometimes inadvertently train their employees to fall for Phish by including links in organisation emails, attaching files that can contain malware, or sending out Word documents with embedded scripts[12]. The company should examine their own practices in this respect and ensure that it is as easy as possible for employees to spot Phishes.
   b) Encourage reporting of emails that people are concerned about. Never make anyone feel bad about reporting emails that turn out to be safe (Murdoch & Sasse, 2017).
   c) Organisations should implement standards such as the Sender Policy Framework (SPF), Domain Key Identified Message (DKIM), and Domain-based Message

[12] https://www.csoonline.com/article/3287655/phishing/stop-training-your-employees-to-fall-for-phishing-attacks.html

Authentication, Reporting & Conformance (DMARC)[13]. Any emails that do not meet these standards should be blocked by the email server, and not delivered to employees.

d) Use certificates so that employees' emails are digitally signed. Then explain to folks how they can confirm the sender of the email in their email client. This makes it so much harder for a Phisher to masquerade as a legitimate employee. This is especially crucial given the fact that Phish emails appearing to come from those in authority are most likely to succeed (Williams *et al.*, 2018).

e) Consider implementing two factor authentication[14]. Then, even if employees inadvertently enter their credentials into a cloned website, the criminals will not be able to use them[15].

2) **Media-Drop:** Provide a safe way for employees to check the contents of USB drives they find. An example is to provide a computer in a shared space: not on the Internet with read-only hard drive. This neutralises the ability of the USB to compromise computers in the organisation so that people can satisfy their curiosity if they find a drive without risk.
3) **In Person:** Consider giving employees access to a tool that will provide them with scripts to use when deciding whether something is an in-person social engineering attack or not (Mouton et al., 2014).
4) **Hygiene**: If displayed or recorded passwords have been found, suggest the company promote use of a Password Manager.
5) **Mobile**: If mobiles access business email, ensure that employees implement access control on their phones.

5. Conclusion
Summary of finding implications

The refined POINTER framework is depicted in Figure 4.

Figure 4: The Refined POINTER Framework

9. Reflection

This research has sought firstly to compile a comprehensive list of techniques used by social engineers. We consulted four sources to do this: (1) research literature, (2) industry reports, (3) hacker activities, and (4) advice offered by official bodies to SMEs. Our review resulted in a list of 12 techniques (*T1-T12*). We then proceeded to compile a comprehensive list of ethical principles which white hat penetration testers can consult to ensure that their activities in this challenging area are indeed ethical (*E1-T17*).

By using the ethical principles to filter those techniques that can be considered unethical, we are left with a set of social engineering techniques that can be included in the PoinTER framework. We then categorised these into five distinct categories: Phish (*T1-T3*), In-Person Attacks (*T8, T9, T12*), Media Attacks (*T5*), Hygiene Tests (*T4*) and WiFi (*T10*).

Although the literature has suggestions for ethical approaches to hacking the human, Faily *et al.* (2015) consider how penetration testers deal with ethical issues. Based on interviews with experienced penetration testers they created a model based on extracting ethical dilemmas and dimensions. Dilemmas were represented by taking either an individual/unstructured position (IU) or a whole/structured position (WS) and the dimensions were represented as Value Ethics, Ethical Appeal, Client Focus and Practice Focus. Through analysis they found fallacies and biases in the model. From this they concluded that decision making

[13] https://engineering.linkedin.com/blog/2018/02/how-linkedin-is-working-to-address-confusion-between-vendor-emai
[14] https://www.clearedin.com/blog/defense-in-depth-anti-phishing-strategies
[15] https://www.businessinsider.com/none-of-googles-employees-get-phished-because-of-yubikey-security-key-2018-7?r=US&IR=T

of the Penetration Testers can be subject to bias and when confronted by ethical dilemmas biases can influence ethical decisions. Hence having a list of ethical principles, as shown in Table 3 and Figure 2, is essential in reducing such bias. Moreover, the filtering of all available techniques, as shown in Figure 3, ensures that only techniques that have been subjected to ethical scrutiny are deployed.

Finally, we propose that a measure of flexibility be incorporated into the framework so that the pentest authoriser can approve or decline specific categories of testing techniques. In so proposing, we mirror practices of many pentesters in industry.

While other authors have written about penetration testing humans, few have produced a comprehensive framework such as this one, which draws its techniques from multiple sources, and subjects each technique to ethical inspection, using a comprehensive list of ethical principles derived from the research literature. This framework is, in itself, a refinement of a previously published framework. We expect further refinements to follow, as this framework is used in the field to guide and inform actual human pentests of SMEs.

10. Conclusion

We report on the refinement of a previously proposed pentest that sought to reduce employee-related vulnerabilities i.e. to improve resilience. Previously, we argued that such frameworks ought to be sensitive to ethical issues and preserve the privacy of the company's employees. In this paper we have further refined the framework based on an extensive review of the academic literature, a review of what hackers exploit and advice from industry with respect to social engineering resistance. Moreover, we provide a list of ethical principles that we used to approve the techniques we included in our framework. This list could equally inform ethical technical pentests.

11. References

Abagnale, Frank and Redding, Stan. 2003. Catch Me If You Can: The True Story Of A Real Fake 23 Jan. Mainstream Publishing (23 Jan. 2003)

Abraham, S. and Chengalur-Smith, I., 2010. An overview of social engineering malware: Trends, tactics, and implications. Technology in Society, 32(3), pp.183-196.

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.

Adewole, A. and Durosinmi, A. 2015. Social Engineering Threats and Applicable Countermeasures. African Journal of Computing and ICT Vol 8. No. 2 pp.177-180

AL-Hamar, M., 2010. Reducing the risk of e-mail phishing in the state of Qatar through an effective awareness framework.(Doctoral Thesis, Loughborough University)

Allsopp, W., 2010. Unauthorised access: physical penetration testing for IT security teams. John Wiley & Sons.

Alvarez, E. 2014. Sony Pictures hack: the whole story. https://www.engadget.com/2014/12/10/sony-pictures-hack-the-whole-story/

Applegate, S.D., 2009. Social engineering: hacking the wetware!. Information Security Journal: A Global Perspective, 18(1), pp.40-46.

Archibald, J. and Renaud, K. 2018. PoinTER: A GDPR-Compliant Framework for Human Pentesting (for SMEs). HAISA. 29-31st August. Dundee, Scotland.

Arenaza-Urquijo, E. M., and Vemuri, P. 2018. Resistance vs resilience to alzheimer disease: clarifying terminology for preclinical studies, Neurology 90 (15): pp. 695-703.

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.

Bauer, Stefan, Edward WN Bernroider, and Katharina Chudzikowski. 2013. "End user information security awareness programs for improving information security in banking organizations: preliminary results from an exploratory study." In AIS SIGSEC Workshop on Information Security & Privacy (WISP 2013), Milano. 2013.

BBC. 2018. Two years for teen 'cyber terrorist' who targeted US officials. 20 April. https://www.bbc.co.uk/news/uk-england-leicestershire-43840075 (http://www.computerevidence.co.uk/Cases/CMA.htm)

Bendovschi, A. 2015. Cyber-Attacks – Trends, Patterns and Security Countermeasures. In Proceedings of 7th International conference on Financial Criminology. Oxford, United Kingdom. pp. 24-31

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.

Beckers, K., Pape, S. and Huck-Fries, V. 2016. Hatch: Hack and Trick Capricous Humans - A Serious Game for Social Engineering. In: Proceedings of the 30th International BCS Human Computer Interaction Conference: Fusion! Poole, United Kingdom — July 11 - 15, 2016

Bowen, B.M., Devarajan, R. and Stolfo, S., 2011, November. Measuring the human factor of cyber security. In IEEE International Conference on Technologies for Homeland Security (HST) pp. 230-235. IEEE.

Brewster, T. 2018. Government Hackers Assault Hundreds Of 'Secure' Google Accounts With Evil Phishes. https://www.forbes.com/sites/thomasbrewster/2018/12/19/government-hackers-assault-hundreds-of-secure-google-accounts-with-evil-phishes/#601652ac1b31

Burkhead, R.L., 2014. A phenomenological study of information security incidents experienced by information security professionals providing corporate information security incident management (Doctoral dissertation, Capella University).

Burton, J., 1979. The Trojan Horse. Leesburg: Adam Smith Institute.

Cameron, D. 2018. Humans Are the Weakest Link: Tales of a Social Engineer. 3 May. https://gizmodo.com/humans-are-the-weakest-link-tales-of-a-social-engineer-1825695781

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.

Castelli, C. Gabriel, B., Yates, J. Booth, P. 2018. Strengthening digital society against cyber shocks. Key findings from The Global State of Information Security Survey. https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/strengthening-digital-society-against-cyber-shocks.html

Castle, S. 2007. Thief woos bank staff with chocolates - then steals diamonds worth €21m. . https://www.independent.co.uk/news/world/europe/thief-woos-bank-staff-with-chocolates-then-steals-diamonds-worth-16314m-5332414.html

Chabrow, Eric. 2008. The Human Factor of Corporate Spying. CIO Insight. June 2008. http://www.cioinsight.com/c/a/Opinion/Corporate-Spy-Story/?kc=CIOMINEPNL06252008.

Chantler, Alan and Broadhurst, Roderic (2006) Social Engineering and Crime Prevention in Cyberspace . Technical Report, Justice, Queensland University of Technology.

Chaudhary, S., 2016. The Use of Usable Security and Security Education to Fight Phishing Attacks.(Doctoral dissertation, School of Information Sciences of the University of Tampere)

Chuenchujit, T., 2016. A taxonomy of phishing research (Doctoral dissertation, Master of Science in Computer Science in the Graduate College of the University of Illinois at Urbana-Champaign).

Cialdini, R. B. “The Science of Persuasion.” Scientific American, Jan. 2001: 76-82.

Cooper, P. 2017.Cognitive Active Cyber Defense: Finding Value through Hacking Human Nature, Journal of.Law & Cyber Warfare, 5(2) p. 57-172.

Curran, D. 2018. My terrifying deep dive into one of Russia's largest hacking forums. https://www.theguardian.com/commentisfree/2018/jul/24/darknet-dark-web-hacking-forum-internet-safety

Dark Reading (2017). Sabre, Travelport Hacker Sentenced to Prison. https://www.darkreading.com/threat-intelligence/sabre-travelport-hacker-sentenced-to-prison-/d/d-id/1329051

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

Dicosmo, A. 2018. Hackers are con artists: The perils of social engineering. https://thenextweb.com/contributors/2018/01/29/hackers-con-artists-perils-social-engineering/

Dimkov, T., Van Cleeff, A., Pieters, W. and Hartel, P., 2010, December. Two methodologies for physical penetration testing using social engineering. In Proceedings of the 26th annual computer security applications conference (pp. 399-408). ACM.

DOGANA, 2016. The role of Social Engineering in evolution of attacks, DOGANA - Advanced Social Engineering and Vulnerability Assessment Framework. https://www.dogana-project.eu/images/PDF_Files/D2.1-The-role-of-SE-in-the-evolution-of-attacks.pdf

Edwards, M., Peersman, C. and Rashid, A., 2017, April. Scamming the scammers: towards automatic detection of persuasion in advance fee frauds. In Proceedings of the 26th International Conference on World Wide Web Companion (pp. 1291-1299). International World Wide Web Conferences Steering Committee.

Eng, J. 2015. Ubiquiti Networks Scam. https://www.nbcnews.com/tech/security/ubiquiti-networks-says-it-was-victim-47-million-cyber-scam-n406201

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

Faily, S., McAlaney, J. and Jacob, C .2015. Ethical Dilemmas and Dimensions in Penetration Testing. In Proceedings of the 9th International Symposium on Human Aspects of Information Security & Assurance, pp. 233–242. University of Plymouth. Faily, S., Jacob, C., and Field, S. .2016. Ethical Hazards and Safeguards in Penetration Testing Proceedings of British HCI 2016 Conference, Fusion, Bournemouth, UK.

Finn, P.R. 1995. Research Ethics: Cases and Materials. In: The ethics of deception in research. P87-118. Indiana University Press.

Fisher, M. 2013. Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism? https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/

Frauenstein, E., 2013. A Framework to Mitigate Phishing Threats (Masters Dissertation, Nelson Mandela University)

Flores, R. W., 2016. Shaping information security behaviors related to social engineering attacks (Doctoral dissertation, KTH Royal Institute of Technology).

Gardi, C., Montanarella, L., Arrouays, D., Bispo, A., Lemanceau, P., Jolivet, C., Mulder, C., Ranjard, L., Römbke, J., Rutgers, M. and Menta, C., 2009. Soil biodiversity monitoring in Europe: ongoing activities and challenges. European Journal of Soil Science, 60(5), pp.807-819.

Goldschmidt, M. 2018. Social Engineering is the new norm in hacking. CSO. 8 March. https://www.cso.com.au/article/634433/social-engineering-new-norm-hacking/

Grinberg, E, and Chavez, N. 2018. Connecticut man sentenced in celebrity photo hacking scandal. 20 Aug. https://edition.cnn.com/2018/08/29/entertainment/celebrity-photo-hacking-sentence/

Hack Story, 2011. Captain Zap, 21 March https://hackstory.net/Captain_Zap.

Hadnagy, C., 2010. Social engineering: The art of human hacking. John Wiley & Sons.

Hadnagy, C. 2014. Unmasking the Social Engineer. Wiley & Sons.

Halevi, T., Memon, N. and Nov, O., 2015. Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks.

Hasan, M., Prajapati, N. and Vohara, S., 2010. Case study on social engineering techniques for persuasion. International journal on applications of graph theory in wireless ad hoc networks and sensor networks. (GRAPH-HOC) Vol.2, No.2, June.

Hinson, G., 2008. Social engineering techniques, risks, and controls. EDPAC: The EDP Audit, Control, and Security Newsletter, 37(4-5), pp.32-46.

Jansson, K. 2011. A Model for Cultivating Resistance to Social Engineering Attacks. Masters Thesis. Nelson Mandela Metropolitan University.

Jeske, D. and van Schaik, P., 2017. Familiarity with Internet threats: Beyond awareness. Computers & Security, 66, pp.129-141.

Kiama, M. 2016. Social Engineering: Managing The Human Element Of Information Security In The Organization. Masters Dissertation, Nairobi University

Kaspersky. 2017. Businesses and personal data: In-depth analysis of practices and risks. https://www.kaspersky.com/blog/data-protection-report/23824/

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

Kennedy, David, O'Gorman, Jim, Kearns, Devon, and Aharoni , Mati. 2011. Metasploit: The Penetration Tester's Guide. No Starch Press.

Klevinsky, T.J., Laliberte, S. and Gupta, A., 2002. Hack IT: security through penetration testing. Addison-Wesley Professional.

Krombholz, K., Hobel, H., Huber, M. and Weippl, E., 2015. Advanced social engineering attacks. Journal of Information Security and applications, 22, pp.113-122.

Labossiere, D. 2015. A Matrix For Small Business Owners To Better Protect Their Network. Masters Dissertation, Utica College

Lanier, C. 2018. Combating Social Engineering: Tips From Black Hat. https://www.bleepingcomputer.com/news/security/combating-social-engineering-tips-from-black-hat-2018/

Laribee, L. 2006. Development Of Methodical Social Engineering Taxonomy Project, Masters Thesis, Naval Postgraduate College, Monterey, California

Larson, S. 2017. Every single Yahoo account was hacked - 3 billion in all. https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/

Lively, C.E 2003. Psychological Based Social Engineering. Global Information Assurance Certification Paper. SANS Institute. https://www.giac.org/paper/gsec/3547/psychological-based-social-engineering/105780 (Accessed 27 Dec 2018)

Liwer, D. 2018. 4 main reasons why SMEs and SMBs fail after a major cyberattack. https://www.csoonline.com/article/3267715/cyber-attacks-espionage/4-main-reasons-why-smes-and-smbs-fail-after-a-major-cyberattack.html

Long, R.M., 2013. Using phishing to test social engineering awareness of financial employees. (Masters Dissertation, Eastern Washington University)

Luo, X., Brody, R., Seazzu, A. and Burd, S., 2011. Social engineering: The neglected human factor for information security management. Information Resources Management Journal (IRMJ), 24(3), pp.1-8.

Mitnick, K. D. Simon, W. L. 2011 The art of deception: Controlling the human element of security, John Wiley & Sons.

Mitnick, K. D. 2018. Tricks and techniques from Kevin Mitnick, the 'world's most famous hacker' 2 Myay. https://www.rappler.com/technology/features/201623-kevin-mitnick-worlds-most-famous-hacker-techniques-epldt-cybersecurity-launch

Mouton, F., Malan, M.M., Leenen, L. and Venter, H.S., 2014, August. Social engineering attack framework. In Information Security for South Africa (ISSA), 2014 (pp. 1-9). IEEE.

Murdock, S., and Sasse, M.A. 2017. Should you really phish your own employees? 15 May. New Statesman. https://tech.newstatesman.com/business/phishing-employees

NCSC (Matt P) 2018. Rating hackers, rating defences. 6 Sept. https://www.ncsc.gov.uk/blog-post/rating-hackers-rating-defences

NCSC (HM Government). 2017. Cyber Security: Small Business Guide. https://www.ncsc.gov.uk/smallbusiness

Nohlberg, M., 2008. Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks. (Doctoral Thesis, University of Stockholm)

Nelms, T., Perdisci, R., Antonakakis, M. and Ahamad, M., 2016, August. Towards Measuring and Mitigating Social Engineering Software Download Attacks. In USENIX Security Symposium (pp. 773-789).

O'Hora, A. 2018. 7 Oct. Jenny Radcliffe: Being friendly could make Irish people susceptible to hackers. https://www.independent.ie/business/irish/jenny-radcliffe-being-friendly-could-make-irish-people-susceptible-to-hackers-37391749.html

Okoye, S.I., 2017. Strategies to Minimize the Effects of Information Security Threats on Business Performance. (Doctoral Dissertation, Walden University)

Olavsrud, T. (2014, December 10). 5 information security trends that will dominate 2015. CIO. Retrieved from http://www.cio.com/article/ 2857673/security0/5-information-security-trends-that-will-dominate-2015. Html

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T. and Ebner, N., 2017, May. Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (pp. 6412-6424). ACM.

Palmer, C.C., 2001. Ethical hacking. IBM Systems Journal, 40(3), pp.769-780.

Paz, H., Vega-Ramos, F. and Arreola-Villa, F., 2018. Understanding hurricane resistance and resilience in tropical dry forest trees: A functional traits approach. Forest Ecology and Management. 426. 15 October 2018, pp. 115-122

Pierce, J,. Ashley, G., and Warren, M. .2006. Penetration Testing Professional Ethics: A Conceptual Model And Taxonomy Australasian Journal of Information Systems 13 (2) pp.193-200

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

Rader, M. and Rahman, S. 2013. Exploring historical and emerging phishing techniques and mitigating the associated security risks. International Journal of Network Security & Its Applications (IJNSA), 5 (4) pp. 23-41.

Rayome, A. D. 2018. The 6 most popular cyberattack methods hackers use to attack your business 3 October. Tech Republic. https://www.techrepublic.com/article/the-6-most-popular-cyberattack-methods-hackers-use-to-attack-your-business/

Resnik, D. and Finn, P. 2018. Ethics and Phishing Experiments. Journal of Science and Engineering Ethics. 24, pp 1241-1252

Robertson, A. 2016. 'Celebgate' hacker sentenced to 18 months in prison. 28 Oct. https://www.theverge.com/2016/10/28/13453166/ryan-collins-celebgate-celebrity-photo-hacker-prison-sentence

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. July 19 – 20. (Article. 52). ACM.

Samtani, S. and Chen, H., 2016, September. Using social network analysis to identify key hackers for keylogging tools in hacker forums. In IEEE Conference on Intelligence and Security Informatics (ISI) (pp. 319-321). IEEE.

Schaeken, M. 2018, Information security awareness measuring & social engineering 2.0. Assessment of information security awareness (ISA) in the Belgian healthcare sector using an enhanced HAIS-Q. (Masters Dissertation, Open University of the Netherlands,)

Security Through Education. Undated. https://www.social-engineer.org/framework/attack-vectors/impersonation/

Slonka, K. 2014. Awareness of malicious social engineering among Facebook users. (Doctoral Thesis, Robert Morris University)

Smith, J. and Shorter, J. 2010. Penetration Testing: A Vital Component Of An Information Security Strategy. Issues in Information Systems Volume XI, No. 1, pp.359-363.

Snyder, C., 2015. Handling human hacking: creating a comprehensive defensive strategy against modern social engineering. (Honors Dissertation, Liberty University)

Spinapolice, M. 2011. Mitigating the risk of social engineering attacks. Masters Thesis. Rochester Institute of Technology.

Stiawan, D., Idris, M.Y., Abdullah, A.H., Aljaber, F. and Budiarto, R., 2017. Cyber-attack penetration test and vulnerability analysis. International Journal of Online Engineering (iJOE), 13(01), pp.125-132.

Stobert, E. and Biddle, R., 2014, July. The password life cycle: user behaviour in managing passwords. In Proc. SOUPS.

Tarallo, H.M., 2015. Social engineering—countermeasures and controls to mitigate hacking (Doctoral dissertation, Utica College).

Tetri, P. and Vuorinen, J., 2013. Dissecting social engineering. Behaviour & Information Technology, 32(10), pp.1014-1023.

Thomson, I. 2017. Crackas With Attitude troll gets five years in prison for harassment. 11 Sept. https://www.theregister.co.uk/2017/09/11/crackas_with_attitude_troll_gets_5yrs/

Thornburgh, T., 2004, October. Social engineering: the dark art. In Proceedings of the 1st annual conference on Information security curriculum development (pp. 133-135). ACM.

Tikkanen, T., Human behavior from CyberSecurity perspective. (Masters Dissertation, JAMK University of Applied Sciences)

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

Toussaint, G., 2015. Executive Security Awareness Primer (Masters Dissertation, Utica College)

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)

Tulloch, M. 2018. 30 May. Social Engineering Attacks: How To Defend Against Them And How To Fight Back. http://techgenix.com/social-engineering-attacks/

US Chamber of Commerce. 2012. Internet Security for Business 2.0. https://www.uschamber.com/CybersecurityEssentials

Von Solms, R., and Warren, M. 2011. Towards the Human Information Security Firewall. International Journal of Cyber Warfare and Terrorism, 1(2), 10-17, April-June.

Walker, L.,Deception of Phishing: Studying the Techniques of Social Engineering by Analyzing Modern-day Phishing Attacks on Universities. (Masters Dissertation, Auburn University)

Whitaker, A. and Newman, D.P., 2005. Penetration testing and network defense. Cisco Press.

Williams. E. J., Hinds, J., Joinson, A.N. 2018. Exploring susceptibility to phishing in the workplace. International Journal of Human Computer Studies. 120, December 2018, pp. 1-13.

Winkler, I.S., 1996, October. Case study of industrial espionage through social engineering. In Proceedings of the 19 th Information Systems Security Conference (pp. 1-7).

WIRED. 2008. Palin E-Mail Hacker Says It Was Easy. 18 Sept. https://www.wired.com/2008/09/palin-e-mail-ha/

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

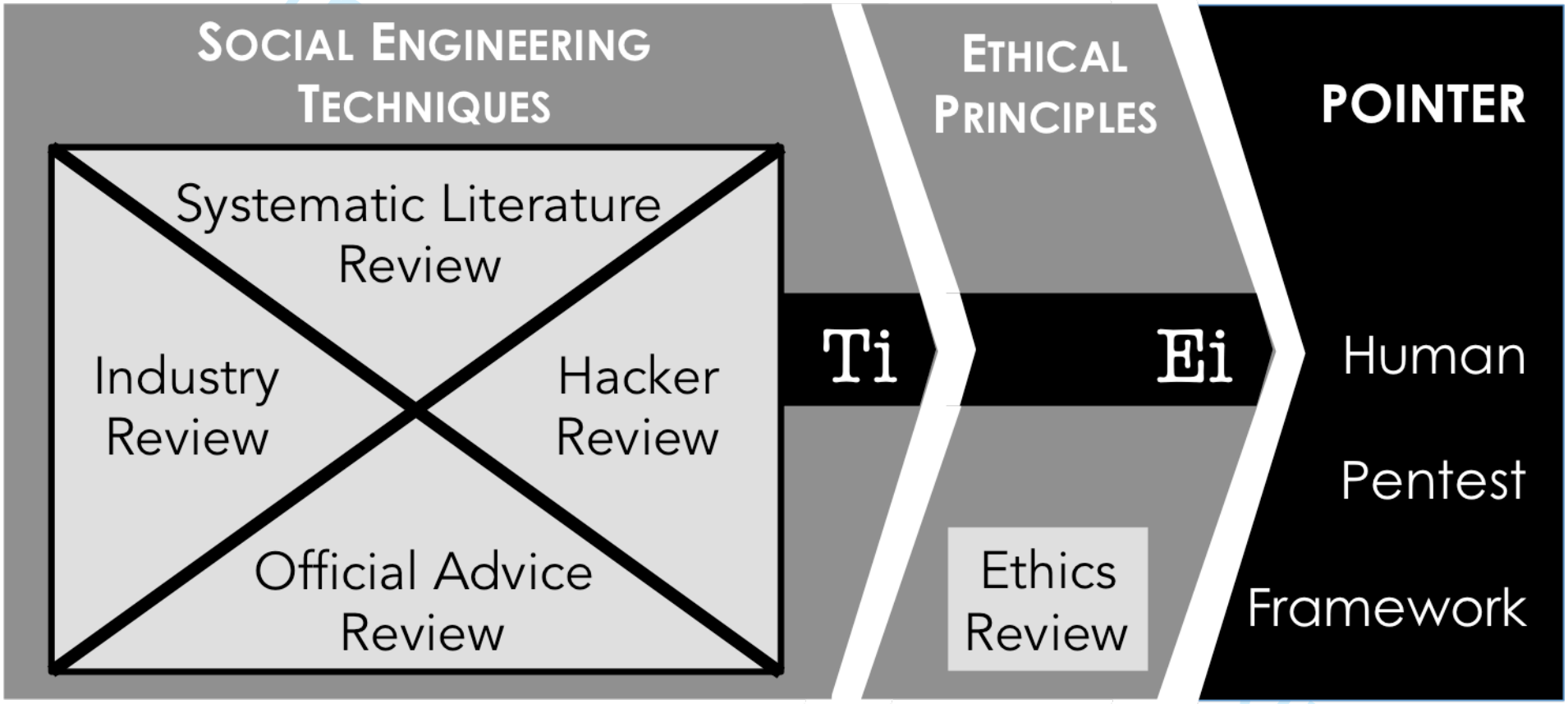
Wright, R.T., Jensen, M.L., Thatcher, J.B., Dinger, M. and Marett, K., 2014. Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. Information systems research, 25(2), pp.385-400.
Yeboah-Boateng, E.O. and Amanor, P.M., 2014. Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5(4), pp.297-307.
Yeo, J. 2013. Using penetration testing to enhance your company's security. Computer Fraud & Security, 2013(4), pp.17-20.
Zetter, K. 2011. Researchers Uncover Rsa Phishing Attack, Hiding In Plain Sight. https://www.wired.com/2011/08/how-rsa-got-hacked/

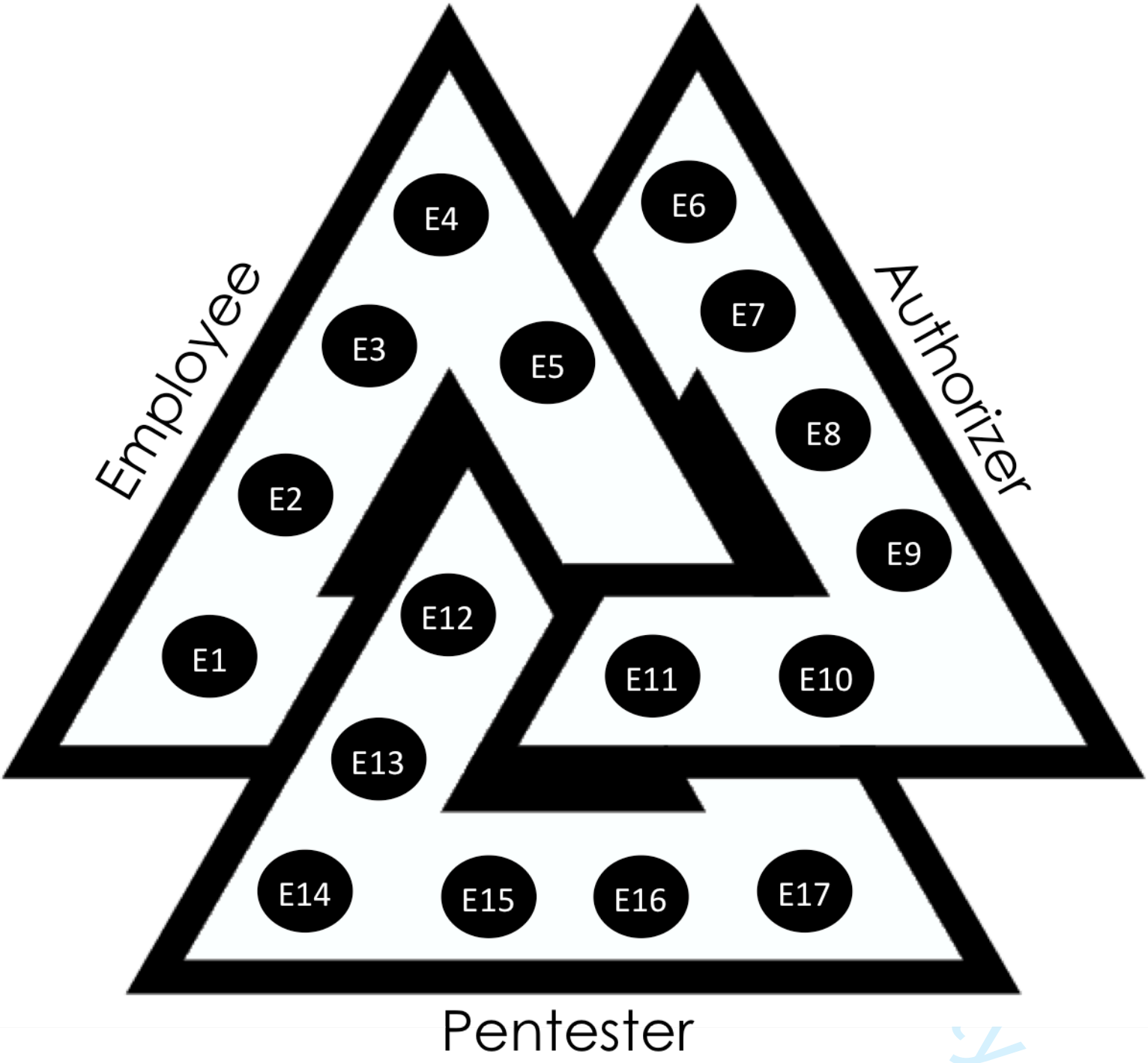
Appendix A: Audit Trail Logbook

Category	Tally	Baseline
Phish	• How many people clicked on link or visited website • How many people reported the phish message	How many Phish messages were sent
Media	• How many times was USB plugged in • How many times USB was reported to manager	How many times USB was planted
In Person	Divulged confidential number Refused to give confidential number	How many calls made
	How many people spotted and reported the keylogger	How many keyloggers were plugged in
Hygiene	Any insecure practices spotted Any secure practices observed	How many times hygiene walk around was carried out
WiFi	• How many connections? • How many times did employees report the rogue WiFi?	How long the rogue WiFi hotspot was available

Appendix B: PoinTER Executive Summary template.

Figure 5: Executive Summary Template


Social Engineering Techniques
Systematic Literature Review
Industry Review
Hacker Review
Official Advice Review
Ti
Ethical Principles
Ei
Ethics Review
POINTER
Human
Pentest
Framework


Employee
Authorizer
Pentester
E1
E2
E3
E4
E5
E6
E7
E8
E9
E10
E11
E12
E13
E14
E15
E16
E17

T1: Phish employees T2: Cloning Websites T3: Ask for Information	**PHISH**	Phishing Simulation (with cloned website for people to visit)
T8: Impersonation T9: Vishing T12: Physical Security	**IN-PERSON**	Try to gain unauthorised access to property by deception. . Vishing: Give employees a confidential number and then get an accomplice to phone and try to persuade them to divulge it
T5: Media Drop	**MEDIA**	Baiting by discarding a USB with software on it that reports installations
T4: Hygiene	**HYGIENE**	Plug in faux Keylogger and see if anyone notices. Look for passwords
T10: Rogue WiFi	**WiFi**	Set up rogue WiFi hotspot and see if employees will connect to it

~~T6: Spear Phishing without Permission~~
~~T7: Guessing Passwords~~
~~T11: SMiShing~~

Unethical
E1-E5,
E13-E15

	PHISH	MEDIA	IN-PERSON	HYGIENE	MOBILE
PREPARE	Email Website	Malware	USBs Phone		WiFi
TEST	◆Scattergun Phish ◆Spearfish with explicit employee permission	Media Drop	◆Elicit Information ◆Media Plug In ◆Vishing	◆Displayed/ Recorded Passwords ◆Confidential Information	◆Access Control ◆Connect to Rogue WiFi
REPORT	Advice	Advice	Scripts	Tools e.g. Password Manager	Advice

COMPANY

POINTER

Time:

Pentest

Tester:

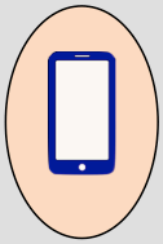
Summary

Phish ☑

Media ☑

Deception ☑

Hygiene ☑



Mobile ☑

Attacks Detected	Likelihood Statistics	Severity Real Hacks
Attacks Succeeded	**Likelihood Statistics**	**Severity Real Hacks**