CHAPTER IX

# Penetration/Intrusion Testing and Vulnerability Disclosure

This chapter looks at penetration/intrusion testing and security-vulnerability disclosure, which, for the purpose of this book, is separated from counterattack/hackback and security activism. The reality, however, is that a response to a security threat may involve aspects of all the above. The differentiation, therefore, serves a point of utility for the structure of the book.

## 9.1 Penetration Testing and Vulnerability Disclosure in Context

Recall that penetration/intrusion testing is a type of information-systems security testing on behalf of the system's owners, also known in the computer-security world as ethical hacking. There is some argument, however, as to whether penetration testing must be done with permission from a system's owner or whether benevolent intentions suffice. Whether permission is obtained or not does not change the common cause, which is improving security.

Most penetration or intrusion testing occurs when a security expert is hired to test the security of an organization's network. In this sense, the security expert has permission to hack into the organization's network such that the law will view this as authorized, thereby not inviting criminal sanction.

In the past few years a mature vulnerability-disclosure and bug-bounty market has come to fruition, though predominantly in

the United States. Vulnerability discovery is the process of finding weaknesses and ways in a network, device, or within the organization themselves that are capable of being exploited by others (sometimes for nefarious reasons). Vulnerability discovery is often done with the authorization of the owner/operator of a network or device, but not always. A bug-bounty market is a program or online platform that pays a monetary sum or benefit (e.g., frequent-flyer points) for information about a systems weaknesses, often in what is known as a software bug.

The legal ambiguity arises when these security experts find security vulnerabilities and actively investigate further without permission or authorization from the system's owner, and then go on to disclose the vulnerability. In this situation, the act would be considered as legally and morally ambiguous, thus qualifying as ethical hacking.

Security activism is similar to penetration/intrusion testing in that the motivation is to improve security. Security activism goes beyond mere testing of security—it works to gather intelligence on crackers and to launch offensive attacks to disrupt criminal online enterprises. This type of reaction is known as counterattack or hack-back and will be explored in chapter 10. A good example of security activism involves botnet tracking and takedown, as will be seen in chapter 11.

When people think of ethical hacking it often conjures images of Anonymous, notable for their use of Guy Fawkes masks. As we saw in previous chapters, movements like Anonymous and the CCC have evolved over the years, garnering a great deal of media attention. The timelines below look at the evolution of some of the protests hacks of Anonymous and the CCC.

Less known are the thousands of other ethical-hacking incidences that occur every day, outside the limelight. One of the most fascinating developments in cyber security has been vulnerability disclosure, bug bounties, and the rise of the marketplace for both. Cyber-security experts are paid to perform penetration testing on networks for various organizations. They also, in their spare time, hunt for vulnerabilities and bugs even in the absence of financial incentive. This has been documented in general of the cyber industry, starting with the open-source-code movement. In 1999, Eric Raymond's *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* was published. In the book, he

describes with exacting precision the culture of computer scientists working together to improve algorithms and the prominent role of reputation in the industry. Penetration testers also shared (and still do in many respects) this ethos. This ethos and the industry as a whole has evolved.

Penetration testers used to predominantly work with a computer emergency response team (CERT) to report vulnerabilities about systems, or they would dialogue directly with affected companies. As will be seen below, this has not always been met with open arms, despite the effort, cost, and diligence expended to find and report the vulnerability or bug. Instead, many researchers have been met with civil suits, threats to prosecute, and, in some instances, prosecution and jail sentences. As a response to the landscape, companies such as Vupen emerged, from which law enforcement and intelligence agencies could purchase licenses to learn about the latest zero-day vulnerabilities. Penetration testers would sell software vulnerabilities to Vupen for financial reward, becoming vendors to the company. After ethical concerns about Vupen began to mount, a different kind of market emerged, whereby the pen tester would submit the bug or vulnerability to a third party—such as HackerOne or Bugcrowd—whereupon such entity would act as an intermediary between the organization and the pen tester. However, as will be seen in the next section, some of the case studies show that such was not always met with appreciation and gratitude.

## 9.2 Timeline

Figure 18 presents a timeline of key vulnerability disclosures.

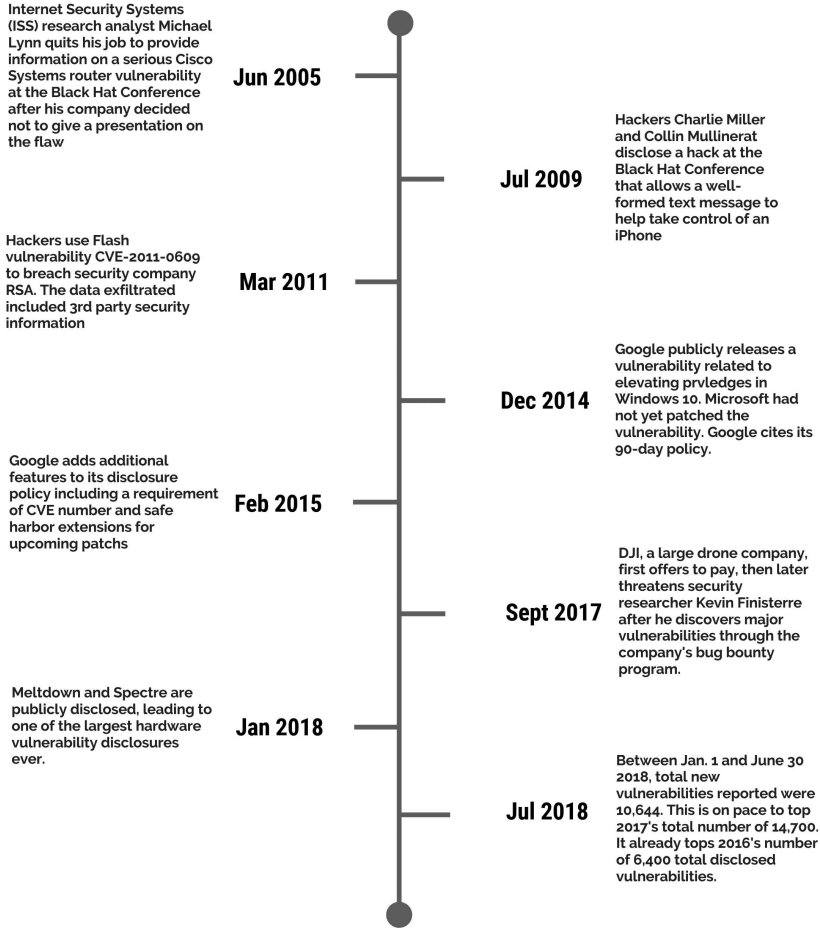


Figure 18. Vulnerabilities.

## 9.3 Case Studies

The case studies for penetration/intrusion testing and vulnerability disclosure are difficult to distinguish as they are closely related.

### *9.3.1 Australian Security Expert Patrick Webster*

Patrick Webster, a white-hat security expert in Australia, was threatened with legal action and criminal charges for disclosing a serious security flaw in an Australian superannuation fund, the not-for-profit First State Super (FFS).[1] When Webster went to log into FFS's system to check on his pension he noticed that the URL contained his individual identity information linking to his superannuation account. He found this odd and investigated further. Patrick ran a simple for loop script to check for other anomalies. The script started with the scan of one account number then continued to scan by incremented numbers. In the time that it took to initialize the script and make tea, the script revealed hundreds of megabytes of account numbers. Upon seeing this, Patrick ascertained that potentially every account was exposed to the Internet. He quit running the program. In the scanning time, the script automatically saved the details of the first 500 accounts.[2]

Alarmed at this security flaw, Webster notified FSS. Some IT personnel sent him emails, thanking him.[3] However, the chief information officer at the fund reacted differently, alleging that by accessing not just his own account but the accounts of others, Webster had committed a crime. Webster was served with legal papers and told that he may face charges, having personally discovered a security flaw that should have been picked up through basic security compliance checks. As a result of the flaw, over 770,000 FSS accounts were vulnerable, as well as the details of another 1.2 million accounts from other companies who outsourced their data storage to Pillar Administration, Australia's largest superannuation administrator. The alarming rate of corporations having their data compromised has sparked data-breach notification laws around the globe. Yet corporations and organizations still have not implemented many basic security mechanisms. At the time, in 2011, FFS was reviewing its data storage contract with Pillar, as well as its own personal handling of personal information.

It has become standard industry practice to thank and often reward those individuals who alert companies to security flaws. Corporations such as Facebook and Google have offered rewards.

Anti-virus and anti-spyware companies also pay money for zero-day vulnerabilities. In this instance, however, FSS's reaction was to threaten Patrick Webster with civil and criminal proceedings if he did not turn his computer over to the IT personnel at FSS for them to verify that he had deleted the information from those 500 accounts.[4] In the end, Webster was not charged and was cleared of any wrongdoing by the Australian privacy commissioner. However, the incident set off alarm bells for security researchers in Australia and elsewhere.

In the words of Webster:

> I am genuinely disappointed the government legislation will not provide safeguards for security researchers, though I am not the least bit surprised.
>
> I've encountered clients who are actively being attacked by a compromised legitimate website and considered counter attacking in self defence to protect my client and the comprised organization.... I haven't, but it would be nice if we could.
>
> My only hope is that my incident with First State Superannuation sets a precedent for future researchers. Obviously not in Australian law as the NSW [New South Wales] Police stated that no laws were broken and I was providing a civil duty, and Minter Ellison [FSS's law firm] halted proceedings, but with any luck the media attention will convince corporations that not everybody is acting with malicious intent. If it helps just one researcher in the future I'll be happy.[5]

The incident is a timely reminder of the lack of legitimate exemptions for security research. After the breaking news of Webster's vulnerability discovery the privacy commission opened an investigation and found that FSS's data security at the time was inadequate.[6]

### *9.3.2 Cisco Router*

There are many renowned international computer-security and hacking conferences, such as Black Hat, DefCon, Hack in the Box, and the CCC. These conferences are unique in that they bring together hackers, crackers (those for criminal gain), white-hat security researchers and experts, as well as law enforcement, and corporate and security

vendors. Many of these conferences have competitions where hackers earn money, reputation, and future clients by identifying security vulnerabilities. Typically the winner will accept the cash prize then hand over their method of exploiting a vulnerability to the vendor. In this sense, the disclosure is limited to the vendor (and perhaps others present at the conference), and allows the vendor the opportunity to patch the vulnerability. In this situation, there is no unauthorized access or use, so threat of civil liability and criminal sanction is very low. Not all conference presentations where vulnerabilities are disclosed, however, have the same happy ending, especially when the vendor has not elicited information about a vulnerability.

The most famous security-vulnerability disclosure occurred during the 2005 Black Hat conference in Las Vegas, where Michael Lynn gave a controversial presentation on vulnerabilities found in a Cisco router. The incident may be the best case study for examining ethical and legal issues surrounding vulnerability disclosure. Most of the Internet's infrastructure relies on Cisco routers. Basically, routers are network devices that forward packets from one network to another. Security researchers have found flaws in Cisco's router software in the past, but typically such flaws were minor, resulting only in a denial-of-service attack. Lynn, then a security researcher with Internet Security Systems (ISS), discovered what is believed to be the first known vulnerability of buffer overflow against a Cisco router. This significant vulnerability would allow an attacker to take over a network. The vulnerability has been described as a potential Pearl Harbour of vulnerabilities.[7]

Lynn's employer, ISS, was in discussion with Cisco about this vulnerability. Cisco was notified that ISS was to present on the router vulnerability at the 2005 Black Hat conference. Cisco's response was to threaten ISS with a lawsuit and demand that the Black Hat organizers remove the presentation from the conference. At this point Cisco had neither fixed the vulnerability (though known to them) nor notified their clients of this potentially serious vulnerability.[8] No patch was available at this time. Instead of backing down, Lynn quit ISS, told the Black Hat organizers that he would present a different talk. But, part way into his presentation, Lynn began to discuss the flaw in Cisco's router. While Lynn did not publish his findings nor display the full vulnerability on screen, the partial descriptions and titbits of code displayed allowed a room full of hackers to fully ascertain and share among themselves the shell code by the end of the presentation.[9]

Cisco filed lawsuits against Lynn and the conference organizers, claiming infringement of intellectual property. There is a research exemption and reverse-engineering right under fair-use (copyright in the United States) and fair-dealings doctrine (in Commonwealth countries), but any publication of the vulnerability afterward may attract copyright sanctions. Copyright infringement can be filed both against the person who publishes (oral presentations included) as well as the distributors—in this case, the conference organizers. The legal suits were dropped against Black Hat and Lynn on the condition that they restrain from future discussion about the vulnerability and the incident in general.

Code that exploits Cisco vulnerabilities often has a substantial market value. Experts have estimated that Lynn could have sold the vulnerability to Cisco at a market value of $250,000.[10] As such, Cisco vulnerabilities are generally not disclosed, even in conferences. Lynn decided to present on this highly important vulnerability due to inaction (some might classify it as a gross lack of action) on Cisco's part to fix the vulnerability once they were notified. Lynn had notified them on several occasions of the vulnerability and had been urging Cisco to fix the problem. Months passed and there was still no action. At this point, Lynn sought to expose the vulnerability to encourage better security practices.

### *9.3.3 LulzSec Hacking to Incentivize Sony to Fix Known Software Bugs*

Arizona college student Cody Kretsinger, allegedly a member of LulzSec, was arrested and charged in the United States with multiple counts of conspiracy and unauthorized impairment of a protected computer for allegedly hacking Sony Pictures Entertainment. The hacking is said to be that of Sony's computer system, which was compromised in May and June 2011. LulzSec, unlike Anonymous, performs hacks both for political reasons and "for laughs" ("lulz" is computer slang for laughs). LulzSec has not formally announced any political reason for the hack. Interesting, however, are the many media comments and blog responses that sympathize with LulzSec, many of which resent the lapse security measures of corporations. As one blogger writes:

> The main offender here is Sony. They were fully aware of the vulnerability of their current system. They were just too lazy to fix it. All it took was a Google search and some script kiddies

> entered in one SQL line and broke into the system. This wasn't a "zero day attack," it was a well known vulnerability to their system that was public. It's like having a stack of money just behind a gate with no lock. All it takes is one simple well known action and you are in. Why do you think class action lawsuits were charged against Sony if it wasn't their fault?[11]

Other members of LulzSec have been arrested and detained in Italy, Switzerland, and the United States for hacking websites. It is much more difficult to see any public benefit or ethical conduct in many of LulzSec's operations, other than the media coverage exposing the poor security habits of corporations and governments. Security experts have been urging companies and governments to improve their outdated and insecure protection of their systems for decades. During the last decade, however, many corporations still do not use basic encryption to protect personal information of their customers, nor do they adequately protect their own assets. The LulzSec attacks may act as a catalyst for corporate improvement to security.

#### *9.3.4 Guardians of Peace, North Korea, and the Sony Pictures Hack*

Since Sony's outing of using hidden rootkits, the corporation has been a favourite destination of attack by hackers since 2006. In 2014, a hacking group calling itself the "Guardians of Peace" released personal and confidential emails from employees of the Sony Pictures film studio. This is referred to as the Sony Pictures hack, as the attack was allegedly in response to the release of the movie *The Interview*, a parody of North Korea's leader Kim Jong-un, perceived in North Korea as disrespectful, even as a threat. This incident could be a case of state-sponsored hacking, which would not fall under our definition of ethical hacking. Nonetheless, I have given it a charitable view. Security experts have stated that the group had been accessing a back door for at least a year prior in Sony's system (it is thought that the back door was used, in addition to a listening implant, proxy tool, destructive cleaning tool, and destructive hard-drive tool).[12]

#### *9.3.5 Vulnerability Hunter Glenn Mangham*

The only criminal-law decision that clearly addresses the role of ethical hacking and security-vulnerability disclosure is the United Kingdom 2012 decision against Glenn Mangham. In *R v Mangham*,[13] Mangham was charged with three counts of unauthorized access

and modification of a computer but was convicted of two counts under the Computer Misuse Act 1990. He was sentenced initially to eight months' imprisonment by the Southwark Crown Court. Later the Court of Appeal (Criminal Division) reduced the sentence from eight to four months due to a lack of malicious intent.[14] Mangham, a university student, took advantage of a vulnerability to penetrate Facebook's firewall. Once Mangham discovered the vulnerability in Facebook's network system, he continued to probe deeper into Facebook's network and, at one point, had downloaded a copy of Facebook's source code. Prosecutor Sandip Patel stated that Mangham, "acted with determination, undoubted ingenuity and it was sophisticated, it was calculating," that he stole "invaluable" intellectual property, and that the attack "represents the most extensive and grave incident of social media hacking to be brought before the British courts."[15] Mangham issued a lengthy public statement regarding the affair, wherein he describes himself as an ethical hacker who had previously been awarded a fee for finding security vulnerabilities within Yahoo.[16] While Mangham takes responsibility for his actions in his statement, he made a number of claims which he felt should have been taken into account. In the past, companies such as Yahoo had paid Mangham for security vulnerability discovery. Mangham had a history of ethical security-vulnerability disclosure. He did not use proxies or anonymizers to shield his identity when discovering vulnerabilities, as his intention was never to use the information for commercial gain. In fact, Mangham had a history of rejecting fees for vulnerability discovery.

This case is potentially interesting for those who disclose security vulnerabilities on a number of grounds. The first is that had Mangham used an anonymizer and proxy server, he could have sold the vulnerability to a security-vulnerability company with impunity. There is no legal requirement for security-vulnerability companies such as Zerodium to verify if a vulnerability has been discovered by breaking the law—most forms of hacking do.

The study of such criminal sanctions for the use of exploits is not central to this chapter but does form part of the legal context in which considerations regarding regulation may occur given that the potential end use may have significant consequences.

### *9.3.6 Da Jiang Innovation*

Da Jiang Innovation (DJI) is a Chinese company that produces the majority of drones worldwide.[17] They announced a bug-bounty program on their website in 2017, offering money for threat identification, and in particular to identify threats relating to users' privacy and vulnerabilities that reveal proprietary source codes of back doors that circumvent safety settings. The specific wording at the time was:

> Rewards for qualifying bugs will range from $100 to $30,000, depending on the potential impact of the threat. DJI is developing a website with full program terms and a standardized form for reporting potential threats related to DJI's servers, apps or hardware. Starting today, bug reports can be sent to bugbounty@dji.com for review by technical experts.[18]

Most other bug-bounty programs contain specific information related to the scope of permissible threat hunting, along with clarification that the company will not pursue civil or criminal suits against the researcher. A researcher by the name of Finisterre was on the open-code platform GitHub, where he found a set of API keys for Amazon Web Services, Amazon's cloud-computing unit, for the DJI source code. API keys are unique identifiers used for authentication. Finisterre used the API keys to access DJI accounts with Amazon Web Services, where he was able to find a series of vulnerabilities. DJI responded with threat of civil suit for going outside of the scope of the bug-bounty program. In the end, a settlement was reached after much negotiation.

## 9.4 Observations

Most people who perform penetration testing and who hunt for vulnerabilities and bugs provide professional services, or they aspire to become recognized as a cyber-security professional. They are motivated predominantly for professional reasons, which include legitimate financial gain, improved employment prospects, and reputation. In my capacity as providing legal information to many cyber-security experts, I would say that they are, by and large, driven to reducing, if not eliminating, security threats, that they enjoy helping others to learn more about cyber security, and, in general, improving the overall cyber ecosystem to make it more secure.

For many cyber-security professionals, in particular penetration testers, it is not enough to be paid to find vulnerabilities and lapse security practices for an organization. They are committed to ensuring that the organization takes action to fix the vulnerabilities. When organizations repeatedly practice lapse security and where they do nothing to fix vulnerabilities where innocent people may be affected, cyber-security professionals become frustrated to the point where they feel an ethical duty to disclose such poor practices. This is similar to many acts of hacktivism where the goal is to assist with the process of reprimanding individuals or groups engaged in harmful activity, such as those who trade in child pornography or are part of criminal gangs, where law enforcement is seen as being ineffective or under resourced. It is a slippery slope, with some forms of ethical hacking becoming acts of vigilantism.

As we will see in the next chapter, actions that "fight fire with fire" may be perceived in many different ways, ranging from acceptable forms of ethical hacking to acts of self-defence, to acts of vigilantism from, as some call them, "cyber-security cowboys."

## Notes

1. Moses 2011.
2. Email correspondence with Patrick Webster 2011.
3. Grey 2011.
4. Grey 2011.
5. Email correspondence with Patrick Webster, 2011.
6. IT Security Training, "First State Super in Breach of Privacy Act' June 7, 2012, available at https://www.itsecuritytraining.com.au/articles/first-state-super-breach-privacy-act. The link to the privacy commission's report has gone dead. See https://www.oaic.gov.au/publications/reports.html
7. Lemos 2005.
8. Zetter 2005.
9. Discussion with a computer-security analyst who was present at the presentation.
10. Lemos 2005.
11. Herpderp1189, *Huffington Post*, January 5, 2012.
12. Lennon 2016.
13. The decision was given in the Southwark Crown Court on February 17, 2012. The decision itself is not reported. Information was obtained through media stories. See BBC News, "York Facebook hacking student Glenn Mangham jailed."

14. *R v Glenn Steven Mangham.*
15. Protalinski 2012.
16. Mangham 2012.
17. With thanks to PhD candidate Rob Hamper for providing me the reference to the DJI case.
18. Da Jian Innovation, "DJI To Offer 'Bug Bounty' Rewards."

Page left blank intentionally