**Part 1**

1.

“The trade – a contract based on future movements in Germany’s Dax stock exchange index – had aroused suspicions because it was far too large for the supposed counterparty, a medium-sized German brokerage called Baader.”

Page 2, FEBRUARY 7, 2008 by Martin Arnold, Peter Thal Larsen, Peggy Hollinger, John O’Doherty and Richard Milne

This specific failing is based on a failure to enforce appropriate access control on the role Jérôme Kerviel had while working at the Société Générale. If this role has better access control it would have been simpler to monitor and restrict the ability of individuals to conduct these kind of erroneous trades. The second paragraph of the sub chapter 5.6.3 details how the role given to an individual account can be used to ensure that a user has the appropriate powers to conduct their duties, and no more. The seventh paragraph details further how Role hierarchies can be used to ensure the relationships between a user and their work can be compartmentalised to prevent unauthorised deals from taking place in the first place. Another technique to detect this type of behaviour would be to have the system automatically flag aberrant behaviour for a human to check.

Chapter 5.6.3 Role-Based Access Control, W. Stallings and L. Brown. Computer Security: Principles and Practice (Third Edition). Pearson, 2014. ISBN 978-1292066172.

2.

“By logging into the system under different names, he then cancelled the fake contracts before they were settled, replacing them with new ones.”

Page 4, FEBRUARY 7, 2008 by Martin Arnold, Peter Thal Larsen, Peggy Hollinger, John O’Doherty and Richard Milne

This failing of computer security principals could have been prevented with a more robust authentication system. By obtaining co-workers passwords through social engineering or other technical means, Jérôme Kerviel was able to cover his own tracks. By having a single sign on system or perhaps biometric systems such as fingerprint scanners, it would have been much more difficult for an individual to perpetrate fraudulent trades under someone else’s name or account. As to how the passwords were initially obtained, it is more likely access to others accounts were obtained from social engineering which could have been prevented with better personal training in conjunction with additional authentication steps such as biometric passwords.

Chapter 4, W. Stallings and L. Brown. Computer Security: Principles and Practice (Third Edi- tion). Pearson, 2014. ISBN 978-1292066172

3.

“Using his knowledge of SocGen’s back office and control systems – a computer system called Eliot – Mr Kerviel was able to enter false hedging contracts to make it appear as if he was taking minimal risks.”

It is possible that access to the part of the system were hedging contracts were stored were granted through the use of malicious software such as a worm. This would have allowed a backdoor into the system which could explain how Jérôme Kerviel was able to amend the files needed to carry out his crime. Regular penetration testing is one way these kind of exploits can be routinely detected. Another precaution which could have helped to more quickly resume regular trading at the Société Générale would be to ensure the log files pertaining to the hedging contracts were properly stored and not tampered with. Keeping track of which user and when, as well as the specific machine has accessed or amended a contract would help prevent a similar situation from reoccurring.

Chapter 6, W. Stallings and L. Brown, Computer Security: Principles and Practice (Third Edition), Pearson, 2014, ISBN 978-1292066172

Chapter 17, D. Gollmann, Computer Security (Third Edition), John Wi- ley and Sons, 2011, ISBN 978- 0470741153 (Chapter 17).

4.

“SocGen also admits it did not change its computer passwords regularly, as standard industry practice requires.”

Enforcing users and system administrators to regularly change passwords is not only best practice, but a failure to do so could also be seen as a breach of the law in its own right. Organisations have a legal and ethical responsibility to take reasonable steps to protect their data and systems. Once a password has been compromised or even suspected to be known and used for malicious intent, it is only detrimental to business proceedings to continue to use this, despite how unpopular mandatory password changing schemes may be with employees and IT staff. The longer a given password is in use, the more likely it is to become compromised in some way, weather through the use of sophisticated technologies or even low-tech shoulder surfing. Additionally, physical security could be improved in which would reduce the possibility of keyloggers or other social engineering techniques from taking place.

Chapter 2, Chapter 19, D. Gollmann, Computer Security (Third Edition), John Wi- ley and Sons, 2011, ISBN 978- 0470741153.

https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-

5.

“He created false e-mails by reproducing the format and header of e-mails he had received from clients, to rebuff any questions from the bank’s internal controls team.”

This type of evasion was a failure of the computer security team to correctly identify a spoofed email. Many browsers and ISP’s have built in antispoofing filters which are capable of detecting emails with manipulated headers and also falsified source addresses for Denial of service attacks. It is possible that these safeguards were turned off or not implemented in the systems at the time the Jérôme Kerviel was conducting his trades. One remedy to this situation would be to devise a system which includes additional verification systems such as a unique hash or private key which could be generated at the time an email is sent. This failure of adequate security procedures could also be rectified with regular face-to-face briefings or a better form of questioning from the internal controls team.

Chapter 7, W. Stallings and L. Brown, Computer Security: Principles and Practice (Third Edition), Pearson, 2014, ISBN 978-1292066172

**Part 2**

**i)**

**Helloworld1.html**

<HTML>

<HEAD>

</HEAD>

<BODY>

<CENTER><H1>Hello World</H1></CENTER>

</BODY>

</HTML>

**iptable1**

iptables -I INPUT -p tcp --dport 25 -m string --algo bm --string ‘hello world’ -j DROP

**ii)**

**helloworld.php**

<html>

<head>

</head>

<body>

<?php

echo "Hello world"

?>

</body>

</html>

**iptable2**

iptables -N w00t

iptables -I INPUT -p tcp --dport 80 -m string --algo bm --string Hello world' -j w00t

iptables -A w00t -j DROP

iptables -t filter –m string "Content-Type: text/html\r\n", "UTF-8" -p tcp -j REJECT

**iii)**

**helloworld3.html**

<html>

<body>

<script>

alert( 'Hello, world' );

</script>

</body>

</html>

**iptable3**

iptables -N w00t

iptables -I INPUT -p tcp --dport 80 -m string --algo bm --string “Hello world” -j w00t

iptables -A w00t -j DROP

iptables -t filter –m string "Content-Type: text/html\r\n", "UTF-8" -p tcp -j REJECT

**iv)**

**helloworldhtml4.html**

<HTML>

<HEAD>

<style>

h1 {

color: powderblue;

}

</style>

</HEAD>

<BODY>

<CENTER><H1>Hello World</H1></CENTER>

</BODY>

</HTML>

**iptable4**

iptables -N w00t

iptables -I INPUT -p tcp --dport 80 -m string --algo bm --string “Hello world” -j w00t

iptables -A w00t -j DROP

iptables -t filter –m string "Content-Type: text/html\r\n", "UTF-8" -p tcp -j REJECT