SOFTWARE ENGINEERING PROGRAMME
UNIVERSITY OF OXFORD
www.softeng.ox.ac.uk

ASSESSMENT

Student: Mayur Pant

Course: Forensics

Date: 14th October 2013

Grade: 80

Gareth Digby; Mark Slaymaker January 20, 2014

Software Engineering Programme
University of Oxford
Department of Computer Science
www.softeng.ox.ac.uk

ASSESSMENT

STUDENT: **Mayur Pant**

COURSE: **Forensics, FOR**

DATES: **14th – 18th October 2013**

GRADE: **80**

REPORT

Your answers to the assignment have demonstrated an excellent understanding of the principles of computer forensic investigation and analysis. Your answers show that you have practiced the processes and procedures taught in the module. Your answers show that you have understood and used the tools and techniques described in the module. Your answers show you have evaluated a computer system in an unfamiliar scenario and discussed your findings in a suitable manner. Your answers show that you have used the tools and techniques described in the module and have a wider understanding of them.

Your have given a good answer to Part 1.

Your answer to Part 2 is very good and comprehensive.

With respect to Part 1
Your answer identifies the phases of a network-based intrusion and provides good descriptions of the phases. You have provided a very good description of the potential evidence of a network-based intrusion that could be recovered from an intruder's computer. You have made excellent use of pictures and tables in your answer.

With respect to Part 2

You have provided very good opinions on the seven questions:

- What had Countess de Rye used the laptop for and how was it setup? Whom, if anyone, had Alexandrine de Rye communicated with using the laptop?
- Did Countess de Rye attack Mr. Pepys' server and if so how?

If Countess de Rye did attack Mr. Pepys' server:

- Was Alexandrine de Rye working for and/or with anyone else?
- Did Alexandrine de Rye deface the blog and if so how?

- Was information on the server viewed or taken (in addition to any viewing of the blog)? Identify the information that has been (or may have been) taken or viewed.
- Was any information passed to a 3rd party?
- If possible identify the location that the attack originated from?

You have identified and made use of a number of pieces of evidence, such as:

- Laptop hostname, issue, timezone
- Laptop users (/etc/passwd)
- User alex's .bash_history
- User alex's mail in .thunderbird/
- User alex's browser history in .mozilla/
- User alex's Metasploit history in .msf4/
- File ~/.ssh/known_hosts
- Files ~/hacks/mail-thread.txt, samuel & mbox
- Files ~/hacks/ pepys.dyndns.org.reconn.txt, user-list.txt, pass-list.txt
- File 200px-Prinsenvlag.svg.png

You have not shown that you have identified and nor made use of a number of pieces of evidence, such as:

- Laptop on/off times (/var/log/messages & syslog)
- Authorizations (/var/log/auth.log)

You have corroborated your evidence by:

- Linking together of auth.log and bash_history for creation of a timeline.
- Linking of Thunderbird email and downloaded server files.
- Linking of Metasploit history with pepys.dyndns.org.reconn.txt, user-list.txt, pass-list.txt.
- Linking together of ssh/know_hosts, bash_history, ssh_host_key_rsa.pub.
- Linking of Firefox browser evidence and the 200px-Prinsenvlag.svg.png graphics file to show the attack.

You correctly identified the two IP addresses associated with the assignment. Three virtual machines (VM) were used to create the evidence for this assignment. The VM for Alexandrine's computer used a VPN so that it appeared to be in the Netherlands at IP address 213.179.209.92. The VMs for Samuel Pepys' server and Queen of Bohemia's emails were both located 96.234.173.244. As mentioned in the assignment there is no need to consider a conspiracy here. The common IP addresses are an unfortunate consequence of the resources available to create the assignment evidence.

For Your Information:
The premise for Part 2 is a server has been used to provide a platform for a blog written by Samuel Pepys and also provide an email service for Samuel Pepys and John Evelyn. The server's **ssh** service has been subject to a brute force attack from an IP address in the Netherlands. The attacker has used usernames and passwords based upon the names of Samuel Pepys and his friends. The Wordpress blog administrative account has also been subjected to a brute force attack. Using the usernames and passwords identified, the attacker makes a reconnaissance of the server identifying the mailboxes of Mr. Pepys and Mr. Evelyn. The attacker then copies the mail boxes off the server using **scp**. The attacker then attempts to deface the blog but realises that Mr. Pepys has not enabled uploading of content; so the attacker enables this; defaces the blog; and finally secures the blog so no one else can upload further material.

Assessor: Gareth Digby **Date: December 29th, 2013**