Information Security (CP3404)

Chapter 15 practical

- This practical consists of some quick quiz questions, tutorial type questions, and hands-on projects relevant to (chosen from) Chapter15 of the textbook (i.e., Mark Ciampa, *CompTIA® Security + Guide to Network Security Fundamentals, Fifth Edition*, USA, 2015).
- You may not be able to complete this practical within the scheduled one-hour practical session for this subject. You are strongly recommended to complete it in your own time (note that you are expected to work 10 hours per week on this subject, including 3 hours of contact time).

Section A – Quick-Quiz/Multiple-Choice Questions:

- Each week, complete the test on LearnJCU within the time allocated, which is before the next practical session.
- These on-line tests are worth 20% of the total marks for this subject.

Section B – Short Answer (Tutorial-Type) Questions:

- Answers to this set of questions are available at the end of this document (Section D).
- Effective learning implies you answer the questions before seeing the answer.

1. List and describe the three categories that TCP/IP divides port numbers into.
2. List and describe two common uses for a protocol analyzer.
3. List four things that a vulnerability scanner can do.
4. Discuss the purpose of OVAL.
5. Describe the purpose of a honeypot.
6. Describe a penetration testing report.
7. List and describe the three (3) elements that make up a security posture.
8. List two (2) types of hardening techniques.

Section C – Hands-On Projects:

Due to security issues, you may not be allowed to practise hands-on projects with university's computers. Interested students are encouraged to do these projects on their own computers (if available). You will not be assessed for utilities/commands that cannot be practised on university computers. Note that you may still be assessed for descriptions/definitions that are provided in this section.

Using Secunia Personal Software Inspector (PSI)[1]

One of the challenges of keeping a system secure is to keep up-to-date on patching software. Although large vendors such as Microsoft and Apple have an established infrastructure to alert users about patches and to install them, few other vendors have such a mechanism. this makes it necessary to regularly visit all websites of all installed software on a system to stay current on all software updates. To make the process more manageable, online software vulnerability scanners were created that can compare all applications on a computer with a list of known patches from the different software vendor sand then alert the user to any applications that are not properly patched or automatically install the patches when one is detected as missing. In this project, you will use the Secunia Personal Software Inspector (PSI) to determine if your computer is missing any security updates[2].

1. Open your web browser and enter the URL secunia.com/vulnerability_scanning/personal/[3].
2. Click **PSI 3.0 Walkthrough**, which is a YouTube video about **PSI**. Click your browser's **Back** button when finished..
3. Click **Download now**.
4. When the download completes, launch the application to install **PSI**.
5. Select the appropriate language and click **OK**.
6. Click **Next** on the welcome screen, then click **I accept the terms of the License Agreement**. Click **Next**.
7. Check the box **Update programs automatically (recommended)** if necessary. Click **Next**.
8. Click **Finish** when the installation is complete.
9. When asked **Would you like to launch Secunia PSI now?**, click **Yes**. Depending upon the computer, it may take several minutes to load the program and its modules.
10. If necessary, click **Scan now**.
11. When the scan is finished, the results will appear like those in Figure 15-8.
12. Applications that can be automatically updated will start the download and installation automatically. On any applications that need manual updates, you can go to the application and then update it.
13. Close all windows[4].

[1] If you are concern about installing any of the software in this project on your regular computer, you can instead install the software in the Windows virtual machine created in practical-1. Software installed within the virtual machine will not impact the host computer.

[2] The current version of PSI contains several advanced features. It supports applications from more than 3000 different software vendors and encapsulate all of the vendor patches for your computer into on proprietary installer. This installer suppresses any required dialogs so everything can be patched silently without any user intervention. You can even create rules, such as telling PSI to ignore patching a specific application.

[3] It is not unusual for websites to change the location of files. If the URL above no longer functions, open a search engine and search for "Secunia Personal Software Inspector"

[4] The Secunia PSI application will continually run in the background checking for updates. If you do not want this functionality on the computer, you can click Settings and uncheck Start on boot.

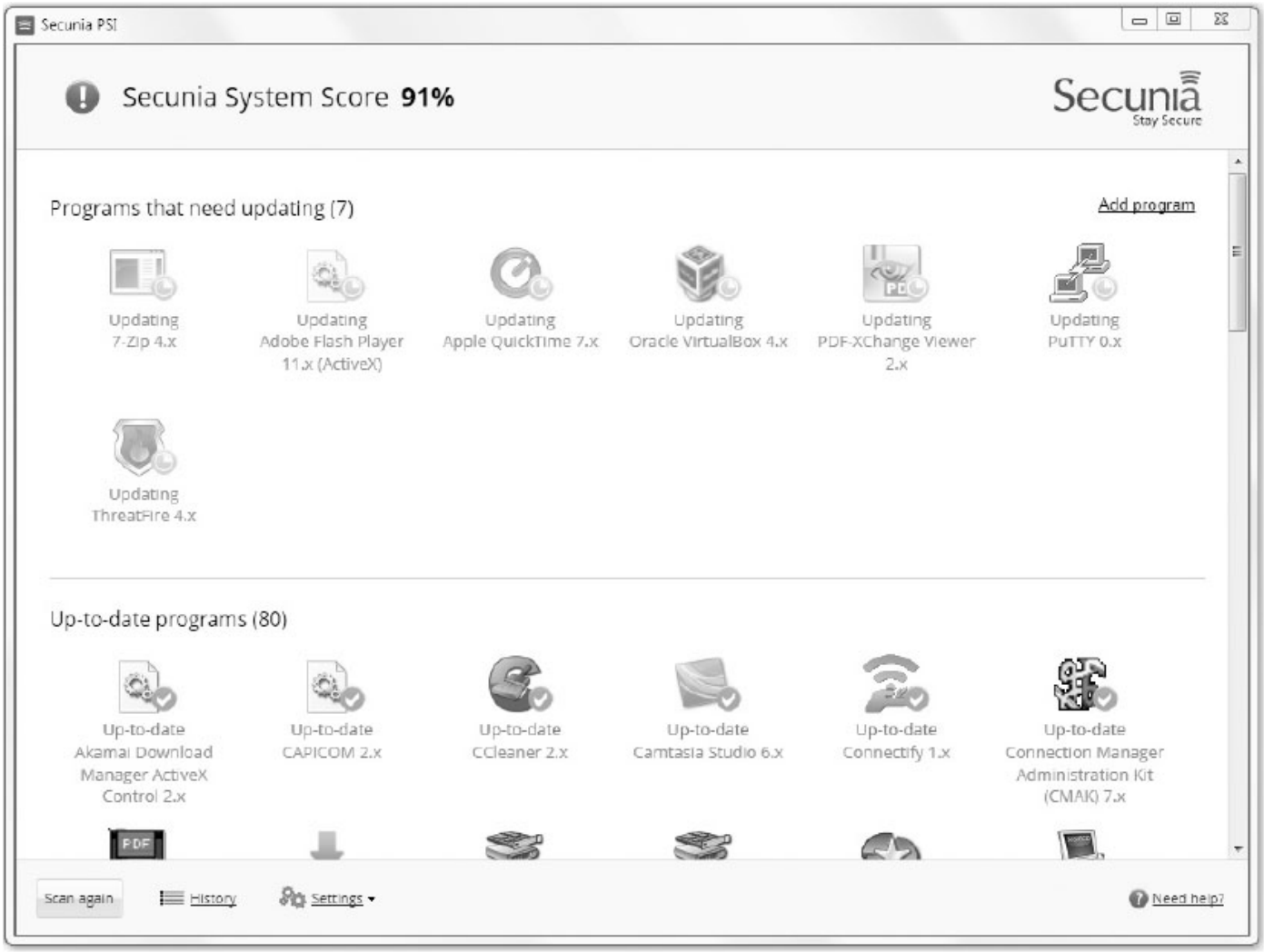

Figure 15-8 Secunia PSI
Source: Secunia PSI

Section D – Answers to Short Answer (Tutorial-Type) Questions:

1. List and describe the three categories that TCP/IP divides port numbers into.

   Answer:
   The three categories that TCP/IP divides port numbers into are:

   (i) Well-known port numbers (01023). Reserved for the most universal applications
   (ii) Registered port numbers (102449151). Other applications that are not as widely used
   (iii) Dynamic and private port numbers (49152 65535). Available for use by any application

2. List and describe two common uses for a protocol analyzer.

   Answer:
   Any two of the followings are fine:

   (i) *Network troubleshooting* – Protocol analyzers can detect and diagnose network problems such as addressing errors and protocol configuration mistakes.

(ii) *Network traffic characterization*– Protocol analyzers can be used to paint a picture of the types and makeup of network. This helps to fine-tune the network and manage bandwidth in order to provide the highest level of service to users.

(iii) *Security analysis*– Denial of service attacks and other types of exploits can be detected by examining network traffic.

3. List four things that a vulnerability scanner can do.

Answer:
Any four (4) items from the followings is fine:

(i) Alert when new systems are added to the network.

(ii) Detect when an application is compromised or subverted.

(iii) Detect when an internal system begins to port scan other systems.

(iv) Detect which ports are served and which ports are browsed for each individual system.

(v) Identify which applications and servers host or transmit sensitive data.

(vi) Maintain a log of all interactive network sessions.

(vii Passively determine the type of operating system of each active system.

(viii) Track all client and server application vulnerabilities.

(iX) Track which systems communicate with other internal systems.

4. Discuss the purpose of OVAL.

Answer:
OVAL is designed to promote open and publicly available security content. It also standardizes the transfer of information across different security tools and services. OVAL is a *common language* for the exchange of information regarding security vulnerabilities. These vulnerabilities are identified using industry-standard tools. OVAL vulnerability definitions are recorded in Extensible Markup Language (XML) and queries are accessed using the database language Structured Query Language (SQL).

5. Describe the purpose of a honeypot.

Answer:
A honeypot can also direct an attacker's attention away from legitimate servers. A honeypot encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server.

6. Describe a penetration testing report.

Answer:
The report is generally *short and sweet*; the main body of the report focuses on what data was compromised, how, and why. The report also details the actual attack method and the value of the data exploited. If requested, potential solutions can be provided, but often it is the role of the organization to determine how best to solve the problems.

7. List and describe the three (3) elements that make up a security posture.

Answer:
The three (3) elements that make up a security posture are:

(i) *Initial baseline configuration* – A baseline is the standard security checklist against which systems are evaluated for a security posture. A baseline outlines the major security considerations for a system and becomes the starting point for solid security. It is critical that a strong baseline be created when developing a security posture.

(ii) *Continuous security monitoring* – Continual observation of systems and networks through vulnerability scanning and penetration testing can provide valuable information regarding the current state of preparedness.

(iii) *Remediation*– As vulnerabilities are exposed through monitoring, there must be a plan in place to address the vulnerabilities before they are exploited by attackers.

8. List two (2) types of hardening techniques.

Answer:
Any two (2) items from the followings is fine:

(i) Protecting accounts with passwords

(ii) Disabling any unnecessary accounts

(iii) Disabling all unnecessary services

(iv) Protecting management interfaces and applications