Unit 8 Assignment

Outcomes addressed in this activity:

- Identify the various types of malware, software exploitation and malicious attack.
- Recognize the symptoms of malware including virus infections.
- Examine the methods available to reduce the threat of malware.

Course outcome:

IT286-4: Examine cryptography methods, vulnerabilities, threats and malicious attacks.

Instructions:

NOTE: You will have two parts to the Assignment in this unit that will be submitted as one file through the Dropbox

Requirements:

Unit Assignments include short essay, descriptive tables and screen captures demonstrating an understanding of the topics. Any resource used including the textbook should be properly cited.

Documents should be submitted using APA Style (double-spaced with a title page and a reference page). Essays should be separated into sections by the Assignment Part number and the question number.

Part 1

1. In a short essay name three ways viruses infect a system and three symptoms that help you identify a virus infection.

2. Create a table that lists and defines five different types of viruses.

3. Research two antivirus products. Create a table that compares the features of the two products. Example: product, systems supported, features, update frequency and cost.

4. In a short essay explain the difference between spoofing, pharming, and phishing attacks.

5) Create a table listing and defining three types of injection attacks.
   Attack   Definition   Defense

6) In a short essay define the following tools that help identify and prevent malware attacks.
   Vulnerability Scanners
   Honeypots and Honeynets
   Port Scanners
   Banner Grabbing
Part 2

Lab Questions and Screen Captures

1. Investigate Ransomware
Ransomware is malicious software that encrypts the hard drive of the PC it infects. The hacker then extorts the PC’s owner in exchange for decryption software to make the PC’s data usable again. Explore this nasty form of malware.

Example:

![Norton Internet Security]

ScarePakage
A ScarePakage variant is targeting more countries: impersonating Europol and AFP
Impersonates legitimate organizations and gets PC user to install encryption software.

![Payment required]

CTB-Locker (Curve-Tor-Bitcoin Locker), Kriptoloker® (new generation) is flagged Critoni.A by Microsoft. Requires payment in Bitcoin.
Visit the DarkReading® website for more information on ransomware. Summarize latest attack. Take screen capture of a ransomware example screen.
Examples:

2. Configure a Phishing Filter

Copyright Kaplan University
NOTE: View the Internet Explorer Security 101 video before you do this lab. A phishing attack is a form of social engineering. In this lab a workstation running Internet Explorer® is required. Internet Explorer®, Internet Options is configured to enable the SmartScreen Filter.

To turn on automatic website checking, follow these steps:
   a. Within Internet Explorer, select Tools from the menu bar, Internet Options and then select the Advanced tab.
   b. Scroll down beneath Settings to Security.
   c. Click Enable SmartScreen Filter. Take a screen capture of the setting. Click OK.
   d. A message appears telling you that website addresses will be sent to Microsoft® and checked against a database of reported phishing websites. Click OK to close Internet Options.

Visit Microsoft’s website and research “How to recognize phishing e-mail messages, links, or phone calls” and the SmartScreen Filter site.

3. View Running Processes in Windows
   This lab requires a Windows operating system.
   Rootkits are not easily discovered because of their ability to hide from the normal reporting of an operating system. One way to determine if a rootkit is present is to use Task Manager to view running processes.

   a. Open Task Manager by right-clicking the Windows Taskbar.
   b. Select the Processes tab and click the checkbox for “Show processes from all users” in order to see the changing total. Stretch out the windows to view the Descriptions. Go to www.liutilities.com/products/wintaskspro/processlibrary to get a list of the common processes that may be running (all systems are different).
   c. Review the values in the CPU column (click the heading to make the highest values show up at the top). The values should total 100, with System Idle Processes showing high numbers. When you open a program (Example: a browser or application) the listing showing the new processes increases. However, if there are high numbers in another process that is not currently running, this may indicate a rootkit. Take a screen capture of the Task Manager Processes tab (the numbers will constantly change). Next, open another application to view a change in the list and take a second screen capture.


Review the grading rubric below before beginning this activity:

Assignment grading rubric = 50 points

<table>
<thead>
<tr>
<th>Assignment Requirements</th>
<th>Points Possible</th>
<th>Points Earned</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Part 1: Essay Questions</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. In a short essay name three ways viruses infect a system and three symptoms that help you identify a virus infection.</td>
<td>0–6</td>
<td></td>
</tr>
<tr>
<td>2. Create a table that lists and defines five different types of viruses.</td>
<td>0–5</td>
<td></td>
</tr>
</tbody>
</table>
## Assignment Grading Rubric

**Course:** IT286  **Unit:** 8  **Points:** 50

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Research two antivirus products. Create a table that compares the features of the two products. Example: product, systems supported, features, update frequency and cost.</td>
<td>0–10</td>
</tr>
<tr>
<td>4. In a short essay explain the difference between spoofing, pharming, and phishing attacks.</td>
<td>0–5</td>
</tr>
<tr>
<td>5. Create a table listing and defining three types of injection attacks.</td>
<td>0–6</td>
</tr>
<tr>
<td>Attack</td>
<td>Definition</td>
</tr>
<tr>
<td>6. In a short essay define the following tools that help identify and prevent malware attacks. Vulnerability Scanners, Honeypots and Honeynets, Port Scanners, Banner Grabbing.</td>
<td>0–8</td>
</tr>
</tbody>
</table>

### Part 2: Lab Questions and Screen Captures

<table>
<thead>
<tr>
<th>Lab Question</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Investigate Ransomware. Visit the DarkReading website for more information on ransomware. Summarize latest attack. Take screen capture of ransomware example. Take a screen capture.</td>
<td>0–3</td>
</tr>
<tr>
<td>2. Configure a Phishing Filter. Take a screen capture of the setting.</td>
<td>0–3</td>
</tr>
<tr>
<td>3. View Running Processes in Windows. Take a screen capture of the Task Manager Processes tab (the numbers will constantly change). Next, open another application to view a change in the list and take a second screen capture.</td>
<td>0–4</td>
</tr>
</tbody>
</table>

**Total (Sum of all points)** | 0–50  |

Less deduction taken for spelling, grammar, and APA errors. Plagiarism is totally unacceptable.

**New total after deductions**

---

Copyright Kaplan University