

Server and Services Security Management Individual Assignment

Objective

To explore, analyse, deliberate and recommend security technology solutions for one of the following cybersecurity threat:

- Fileless Malware
- Cryptojacking Malware
- Spectre/Meltdown Malware

ICA Weightage: 10%

Instructions

1. This is an individual assignment.
2. Each student to choose **ONE (10) of the above threats** to brainstorm and analyze before writing the report. The overall assessment for the assignment is 10%. You must choose from one the following: (a) Fileless Malware, (b) Cryptojacking or (c) Spectre/Meltdown, which should have had some knowledge after watching the videos during Week 3 SDL Week.
3. Research the threat. **You MUST download one reference from Gartner Research** to help support or elaborate the topic that you have chosen. It could be to help explain a technology solution to the problem, or describe what is the problem.
4. The study must include 4 sections: the description, nature of threat and threat mitigation and conclusion.
 - a) Description: What is the cause of the threat? Why is it a threat?
 - b) Nature of threat: What are the potential threats faced by online users? Provide more information about the threat e.g. date launched, the damage caused by the threat, who are the affected users etc...?
 - c) Threat mitigation: Provide recommendations on how the threat can be avoided, minimized or controlled?
 - d) Provide an overall conclusion to the threat.
5. Write a report in MS Word document (Between 500-1000 words). The report **MUST** provide references using hyperlink tags to web sites. As mentioned in **point 3**, one of the references must be from Gartner. Please refer to Blackboard on how you can use Gartner Research through our Library. To use Gartner, do the following:
 - a. Login to NYP Library Portal (<https://library.nyp.edu.sg>) using your student account
 - b. Click myResources

myLibrary Account

myAlerts

myServices

myResources

myLinks

myForms

▶ 3 items on loan

▶ 0 items overdue (Fines for onloan items : \$0.00)

c. Click Databases

myLibrary Account

myAlerts

myServices

myResources

myLinks

myForms

▶ Databases

▶ E-Books

d. Agree to the Terms and Conditions

e. Click on Information Technology

Resources | Databases

Databases

Browse Databases by:

Title List

A - E | F - P | Q - Z

Category List

▶ 123rf

▶ Design

▶ Engineering

▶ Health Sciences

▶ Chemical & Life Sciences

▶ Education

▶ General

▶ Information Technology

f. Click on Gartner Core Research

Information Technology



Gartner Core Research
(Unlimited Concurrent Users)

▶ More Info

+ FAVOURITE

Share

0


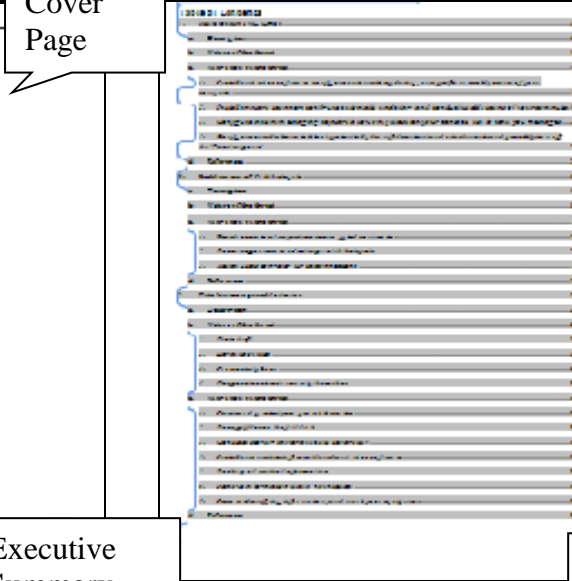
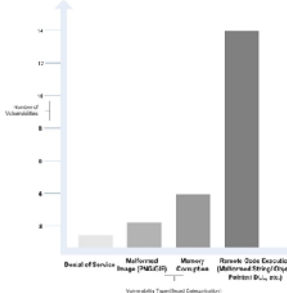
6. You are expected to organize, elaborate and expand on the threats.
Reports with large portions copied from the original reference will not gain any marks.

7. Submit your report (in soft copy) through **Blackboard Turnitin** by the end of Week 12. The due date is **Sunday, 1 July 2018 by 11:59pm**. Late submissions will incur a penalty of 5% of total ICA marks **per day**.

Report Outline and Marking Scheme

- | | |
|--|------------|
| 1. Cover Page and Index | (10 marks) |
| 2. Executive Summary (A short intro of your report, 1 or 2 para) | (10 marks) |
| 3. Report Formatting | (10 marks) |
| • Main Content | |
| • Description of Threat | (10 marks) |
| • Nature of Threat | (20 marks) |
| • Mitigation of Threat | (20 marks) |
| • Conclusion | (10 marks) |
| 4. Text References | (10 marks) |

Pages of Sample Report

<p>Cover Page</p> 	<p>Index Page</p> 										
<p>Executive Summary</p> <p><u>h. Executive Summary</u></p> <p>The current network of the local game production company has a simple network setup and it uses NAT Router to facilitate security into and out of the network. With the proposed network solution it can help the game production company to overcome security threats so that it will not affect the sales and connections with business partners, remote laptops, kiosks, smart phones, and other mobile devices when doing e-commerce.</p> <p>The internal server consists of primary server, application server and workstations to connect its internal network to the internet. To facilitate B2B transaction processing, DNS, mail server and web server are being added to the network. Internal firewall denies all IP address and only allows its own servers to access its trusted zone. External firewall in DMZ permits all IP address and access from the public (untrusted zone) PCs, remote laptop, smart phones and kiosk to access the email server web server and DNS.</p> <p>When doing e-business, e-commerce security is highly threatened. There will be a high risk of forged instruments with disputed charges and insufficient funds in customer's account and unauthorized redistribution of purchased items. Stolen credentials or password of the public will lead to hackers to steal or delete data. Transmission security such as passive sniffing, active spoofing, masquerading and denial of service bring network to its knees. ActiveX and Javascript will actually read data and vulnerable to attacks while eavesdropping and fraud will affect both public and organization. Sometimes, cyberstalkers may also register a domain name that is trademark of some company's name in hope that the organization will pay huge dollar amounts to acquire URL. Registering public key, having digital signatures and digital certificates are recommended for the game production company to help them solve those problems.</p> <p>On top of that, employees should keep their laptop up-to-date personal firewall software, anti-virus, and anti-spyware and also on other computer systems in the organization and do not let employees block defenses and allow malicious third-party tools to enter the system. They should also not install IM and do reckless web surfing like going to social networking sites, porn sites, casual gaming sites, celebrity sites or open malicious email links during working hours. The company should set up firewall; network administrator should change administrator passwords and have back-up plans.</p> <p>Insider attacks are more dangerous because intruders have the access and knowledge necessary for corruption. By implementing the principle of dual control, every key resource of that organization has a fallback. Many companies lack of contingency planning policy or disaster recovery plan, leaving their business slow to recover and restart operations. If the organization has enough money, hire an expert to help develop sound information assurance methodologies. Inexperienced or underfunded companies often install routers, switches, and other networking gear without involving anyone who understands the security ramifications of each device. Therefore, perform an automated vulnerability audit scan is vital.</p>	<p>Main Content and Text References</p> <p>IT2757 Info-Security Group Assignment</p> <p>10. E-Commerce Threats</p> <p>Target sector: merchants of fashion, upscale regional retailers with no same domain name for DDD and Twitter accounts. Users are tricked into revealing their sensitive information, as well as making online transactions. These businesses that do business with you will be attacked you. If this happens to your company, credit card information will be submitted to the hackers instead of you. Imagine ending a loss and having to subsidize your customers!</p> <p>11. Microsoft Office Loopholes</p> <p>Since your company utilizes Microsoft Office Suite heavily, you ought to know the vulnerabilities. Below is a figure that shows the highest vulnerability type.</p>  <table border="1"> <thead> <tr> <th>Vulnerability Type/Component</th> <th>Number of Vulnerabilities</th> </tr> </thead> <tbody> <tr> <td>Default of Service</td> <td>1</td> </tr> <tr> <td>Malformed Image (PNG/JPEG)</td> <td>2</td> </tr> <tr> <td>Memory Corruption</td> <td>4</td> </tr> <tr> <td>Remote Code Execution (Malformed String/Offset Pointer ROP, etc.)</td> <td>14</td> </tr> </tbody> </table>	Vulnerability Type/Component	Number of Vulnerabilities	Default of Service	1	Malformed Image (PNG/JPEG)	2	Memory Corruption	4	Remote Code Execution (Malformed String/Offset Pointer ROP, etc.)	14
Vulnerability Type/Component	Number of Vulnerabilities										
Default of Service	1										
Malformed Image (PNG/JPEG)	2										
Memory Corruption	4										
Remote Code Execution (Malformed String/Offset Pointer ROP, etc.)	14										