|  |
| --- |
| Description: Description: RMIT logo 35mm colSchool of Computer Science and Information Technology |
| Security in Computing and IT  Assignment  Semester 2, 2017 |
| Student First Name STUDENT LAST NAME |
| Student ID |

DECLARATION AND STATEMENT OF AUTHORSHIP

1. I hold a copy of this work which can be produced if the original is lost/damaged.
2. This work is my original work and no part of it has been copied from any other student’s work or from any other source except where due acknowledgement is made.
3. No part of this work has been written for me by any other person except where such collaboration has been authorised by the lecturer/teacher concerned.
4. I have not submitted this work previously for this or any other course/unit.
5. I give permission for this work to be reproduced, communicated, compared and archived for the purpose of detecting plagiarism.
6. I give permission for a copy of my marked work to be retained by the school for review and comparison, including review by external examiners.

I understand that:

1. Plagiarism is the presentation of the work, idea or creation of another person as though it is my own. It is a form of cheating and is a very serious academic offence that may lead to exclusion from the University. Plagiarised material can be drawn from, and presented in, written, graphic and visual form, including electronic data and oral presentations. Plagiarism occurs when the origin of the material used is not appropriately cited.
2. Plagiarism includes the act of assisting or allowing another person to plagiarise or to copy my work.

(https://www.rmit.edu.au/students/student-essentials/rights-and-responsibilities/academic-integrity)

# Task 1 Vulnerabilities and Malware

## Task 1.1 CVSS

1. **Criticality level**

High

1. **Impact**

**CVSS Score:**

7.5 (AV: N/AC: L/PR: N/UI: N/S: U/C: H/I: N/A: N)

**Vulnerabilities:**

Lead to information leak

1. **Purpose of using CVSS scores**
2. To scale which vulnerability should be fixed first.
3. To pre-protect the system from potential attack
4. **Solution**
5. Do not install application from unknown resource
6. Do update on time
7. **Australian DSD Strategies can be applied**
8. This vulnerability is an android-targeted vulnerability:

So:

Patch operating system

1. Because its attack vector is by network

So:

Block spoofed emails

1. For vulnerability type is information leak

So:

use application whitelisting to help prevent malicious software and unapproved programs from running which can avoid critical info be retrieved by malware

**Task reference page:**

<https://nvd.nist.gov/vuln/detail/CVE-2017-12817>

## Vulnerability analysis

### Recent vulnerability

1. **Critical level**

High

1. **Impact**

**CVSS Score:**

7.8

**Vulnerabilities:**

Web Sockets can be exploited remotely to cause denial of service.

Embedded frames can be exploited remotely to obtain sensitive information

Memory corruption vulnerabilities can be exploited remotely to execute arbitrary code

1. **Solution:**

Update to the latest version of thunderbirds

1. **Australian DSD Strategies can be applied**
2. For this is an application’s vulnerability

So

patch applications

1. For this vulnerability may cause DDoS attack

So

Network Segmentation and Segregation is needed to separate physical links and systems and apply traffic flow filters

1. **Task reference page:**

<https://threats.kaspersky.com/en/vulnerability/KLA11090>

### Threats

1. **Threat 1 “BACKDOOR.WIN32.ACKCMD”**
2. Attack strategy

Deception

Downloads

1. Target

Get sensitive information

Redirect page to advertisement page to get money

1. Hiding methods

data will be transmitted directly using ACK packets. This makes it possible for the Trojan to bypass some firewalls.

1. Task reference page:

<https://threats.kaspersky.com/en/threat/Backdoor.Win32.AckCmd>

1. **Threat 2 “Trojan-FHNH”**
2. Attack strategy

Downloads

Attachments

1. Target

Harvest bank information to get money

1. Hiding methods

Inject registry keys in to system

1. Task reference page:

<https://www.mcafee.com/threat-intelligence/malware/default.aspx?id=9609534>

1. **Threat 3 “Trojan.Starloader”**
2. Attack strategy

Deception

Downloads

1. Target

Get sensitive information

Get more victim computers

1. Hiding methods

Hide itself as a jpg file

1. Task reference page:

<https://au.norton.com/online-threats/trojan.starloader-2017-092904-4221-99-writeup.html>

## Task 1.3 Security incident analysis

1. **Pre-condition:**

One of major cyber-attack method:

Malware

Kill chain of Malware:

1. **Reconnaissance**

Define what to get from an end-user, like game account, bank account info, or a bot computer, etc.

Find available vulnerabilities from a OS or a specific software.

1. **Weaponization**

For professional Hackers

Write virus or worm which targeted at exploit the vulnerabilities and get what they want.

Sometime combine the malware with some piracy software (like some game, or MS office)

For Career criminals

Pay money to professional programmers to get the malware they want.

1. **Delivery**

Method 1: Get a fake official company’s domain, like microsfot.cc, etc., and send fake official company email with malware to seduce victim to download it. (Target will be the users of this company’s user)

Method 2: Publish as a resource on a P2P share website, to let others download. (Target will be some game player or those who want free software)

Method 3: Social Engineering

1. **EC**

Method 1: Malware triggered by user after being download

Method 2: Triggered by a spy in a company or an organization

1. **Installation**

Backdoor setups automatically by the malware automatically to protect itself.

1. **Actions on Objective**

Automatically gather info and send back, or run the command/application the intruder required

# Task 2

## Subheading

1. **The plain text**

ZhangLLLLLLLLLL

1. **The three letters**

SIC

1. **Final message**

SICA NSJT SEVR HGOW AB

1. **Final ground setting**

WAH

# Task 3

## Subheading

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Packet filter | X.509 certificates | sandboxing | RAID |
| Key loggers | Partially effective, because once key is logged, data need to transfer out may be by net, packet filter can defend that, however if there’s a backdoor, packet filter won’t work | Not effective, X.509 is a kind of cryptography, normally for secure communication and Signature cannot defend logging at all | Partially effective, for Key loggers have two types, one is software-based, another one is hardware-based. Sandboxing is effective for software-based one, sandbox can control the software access abilities to system resources and internet. However, if hardware-base, sandboxing cannot do anything to prevent logging operation | Not effective, RAID combines multiple physical disk drive components into a single logical unit for the purposes of data redundancy, performance improvement. So, it will do nothing for logging |
| Spyware | Partially effective, this can defence or blocking sensitive information packets sending out or command transferring in. However, there’s a backdoor, this will fail to work | Partially effective, with X.509, information of user is communicating with others can be protected. However, this cannot protect local information and sensitive data | Very effective! The access of spyware to local data and network is strictly controlled. Unless it is authorized by administrator, all things are protected! | Not effective, cannot block Spyware to local sensitive data at all. |
| CPU/resource stealing | Not effective, normally CPU/resource stealing is done by local malware, packet filter cannot do anything | Not effective, X.509 targets at protect network communication and Signature, so X.509 cannot do anything to this attack | Very effective! The resources of malware are all controlled by sandbox, including CPU and other resources, so, it is very effective. | Not effective, RAID only can protect local data however cannot defending CPU/ resource stealing |
| Poisoned search results | Partially effective, normally poisoned search results cannot be blocked by filter directly poisoned search results only can be defended after some users have already being attacked or someone find the poisoned results. | Not effective, cannot do anything when poisoned search results attack happens. | Not effective, poisoned search result is a remote page or application to deceive sensitive information. All operation cannot control by sandbox | Not effective, poisoned search results is controlled by remote search company, RAID just protect local info |
| Clickjacking | Partially effective, can be filtered but also can be defended after some users have already being attacked or someone find this clickjacking | Not effective, only can ensure protected communication with others. However, cannot find out clickjacking attack | Very effective, it is very effective and adaptive in daily life. Browsers, like chrome, use sanding box mechanism. When browser find it is a clickjacking attack, sandbox can roll back or prevent next operation. | Not effective, cannot do anything when clickjacking attack happens |
| Phishing | Partially effective, though phishing page can be filtered however, it only can be filtered after some users have already been attacked | Partially effective, normally big company have X.509 certificates which is issued by trusted CA Publisher to protect communication between website and user and can be used to verify whether this is an official website. However, this sometime ignores by users | Not effective, sensitive always send actively by users, which cannot be protected by sandbox | Not effective, only protect local data, no use for remote fake page or app |
| Password cracking | Very effective, direct password cracking need tons of times’ requests so it can be detected by filter and defence it. | Partially effective, if a local password is encrypted by X.509 certificate and the private key is secure. The password is hard to be find out. However, when it is a website’s password. X.509 can do nothing to protect passwords. | Partially effective, prevent untrusted process, remote request to access local resource so that local password cannot be cracked. However, online one can hardly be protected by sandbox | Not effective, can do nothing when a cracking is processing. |
| Statistical inference attack | Partially effective, can reject untrusty request, but hardly to prevent from internal statistical inference attack | Not effective, only can ensure info security while transferring, cannot prevent Statistical inference attack | Partially effective, can restrict access to sensitive info so that statistical inference attack cannot start. | Not effective, can do nothing when inference attack start. |
| Ransomware | Partially effective, can prevent ransomware after some attacks have already happened but almost ransomware cannot be preventing previously. Also, some ransomware can be transfer by physical hardware like u-disk. | Not effective, even can be used by ransomware to lock local data and almost have not method to unlock without attacker’s help like “wannaCry” | Very effective, almost all resource is protected and cannot be accessed nothing local can be affected. | Partially effective, it has file redundancy and copy of another disk. Some data can be rescue. However, if hackers get some sensitive personal info, RAID can do nothing to help that. |