Assignment2 Design, implement and test substantial scripts to solve problems in Computer Security, Networking and Digital Forensics. A portfolio of programming tasks and tests designed to assess various aspects of computer programming and scripting

Student Username: da5crt

Student ID:2010836

This report will evaluate the risks, monitor and represent the common threats for big organisations in our present and foreseeable cyber space environment, point out vulnerabilities and also bring down to the attention of the receiver of this document effective techniques, solutions, implementation methods and ‘tactics’ to prevent, protect, defend and secure the agency’s resources in order to achieve a stable CIA triad concept (confidentiality, integrity and availability).

The risk is the potential of loss/damage of data assets or information. It fluctuates depending upon external and internal factors. There are vast expanding number of risks daily, but the list of the most common ones is

1. Malware-unwanted piece of program disrupts by installing itself undercover causing unusual behaviour of our system (deleting, stealing, editing, or spreading). Recent research of Luke Irwin (IT governance 2021 27th May) and many examples like NHS (2017), Eurofins Scientific (16/08/2019 BBC News, By Danny Shaw)
2. Traffic interception(eavesdropping)-third party is ‘’listening’’ or manipulating information between users and hosts
3. Phishing attacks – simple method that has been around the IT sector for some time effectively gathering access or stealing sensitive information attacking the human factor in the process via sending emails with links to suspicious websites
4. DDoS attack (Distributed Denial of Service) – the way devices communicate over the network is with acknowledgments and requests. This is a type of an attack, which overload the capacity of our system receiving request which leads to shutting down the server or deliver a very low performance
5. Cross Site Attack (XSS) - third-party will infect a vulnerable website that a regular user interacts with to steal user’s data or disrupt or corrupt services
6. Water Hole Attack – real-time threat where a group of attacking devices will corrupt many websites that certain organisation uses in manner to load a malware software from the infected websites to organisation’s machines. Good example of it is back in 2013 with Department of Labour back in 2013 (Lastline 25 Apr 2019)
7. Drive-by attack -code containing malicious script and it is delivered on our system with no interaction needed by the user
8. Ransomware- encrypting system data and asking for ransom in order the user to obtain the lost assets of information back. Recent example of it was Atlanta’s 2018 government ransomware attack (A Cyberattack Hobbles Atlanta, and Security Experts Shudder, New York Times 2018/03/27)

Due to Kenna Security (2021) all those threats, causing endless stream of malware crossing the network, trying to find the vulnerabilities of our network and mission is to corrupt our system, are growing bigger and getting more sophisticated daily. The need for a constant review and daily updates its crucial to reach a stable environment, which our goal is, too. This report will focus on the three most alerting problems in our vision and propose ways to preventing any future implementation to bring the security on a high level for the government organisation. They are:

* Water Hole Attack

Infected Website

Compromised Server

Cyber-Attacker Device

Government Agency

Infected Website

Compromised Server

Cyber-Attacker Device

Infected Website

Compromised Server

Cyber-Attacker Device

-Redirected Script

-Connection with the website

According to [www.fortinet.com](http://www.fortinet.com) (What Is a Watering Hole Attack? | Fortinet, 2021) the must few steps reaching satisfactory level of protection against this kind of threat are:

A) Regular security testing (pen test)

B) High-level Threat protection (behaviour analysis)

C) Up to date software and system

D) All traffic should be untrusted, and user must be denied access

E) Test and secure against exposure. Many companies offer secure web gateway, which services have HTTPS inspection, remote browser isolation, URL filtering deliver, data loss prevention and app control. All crucial for effective safe fundaments.

* Ransomware

In this case the only way not to fall in a situation of encrypted data and the organisation to be ransomed for its own possessions preventative detection is the best way keeping it safe. Due to Mike Loukides (10/08/2021 O’Reilly) the best way defending against ransomware is the basic security hygiene which will involve : nontrivial passwords (changing),2 factor authentication ,social engineering with training staff to recognise potential phishing, physical backups that tested on a regular basis, keeping OS up-to-date, implementing Samba (Linux) and Active directory (Microsoft) will give permission only to people who need it them and ABAC(attribute-based access control) will give the essential prepared defence, also firewall and good anti-virus will prevent intrusion from a 3rd party.

Start detection

Access directory

Class the file

.doc

.ppt

.pdf

Calculate entropy value

Value

Ransomware holding

Database

Ransomware type

Entropy value

Accuracy

Error rate

Tracing encryption

Suspected Ransomware (Y/N)?

File read, write log analysis

N Y

* DDoS Attack

According to Chinese team of experts( www.hindawi.com 2017) and a survey that they overview ,the low-based DDoS are the new threat .Much easier to detect high-rated threats are more predictable and can be managed ,but the real danger comes from the low-rated DDoS attackers ,who exploits the vulnerability of TCP periodically sending burst attack packages staying under the radar and avoid being detected by any detection script ,simply because it is very hard to distinguish from the legitimate traffic. A packet size detection approach that is suggested by above mentioned is a very good way of defending the organisation. It can be expressed in this flowchart:

Start

Input scanned traffic, packets and network flows

Time is less or equals time intervals

Y

N

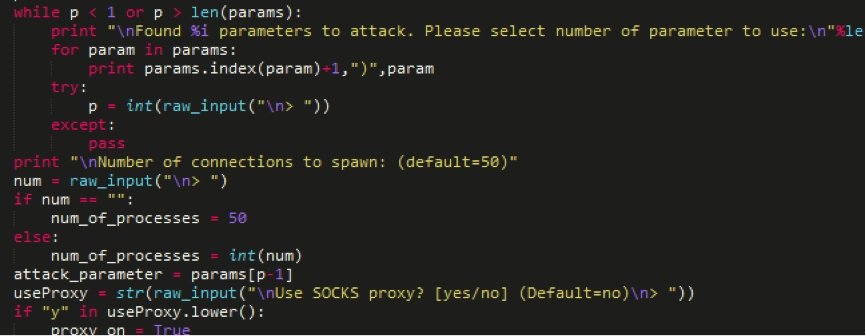
Algorithm and methods

Calculate the mean packet size

N Y

Raise low-rate DDoS attack alarm

This is an example of RUDY (R-U-Dead-Yet) -this attack script for example slowly opens several connections and tries to keep them open as long as possible and guarantee more requests been send (Imperva 2021)



Regardless those preventative measures and methods, detecting preventing and protecting the agency will be needed and delivered using some exception handling to manage any special events while the program runs (Definitions and Hope, 2021), so we can cut or continue some certain process. Exception handling needs to be not only used but also captured in the software we use:

|  |
| --- |
|  |
| **import 'dart:io';** |
|  |  |
|  | **import 'package:dio/dio.dart';** |
|  | **import 'package:flutter/foundation.dart';** |
|  |  |
|  | **const \_defaultConnectTimeout = Duration.millisecondsPerMinute;** |
|  | **const \_defaultReceiveTimeout = Duration.millisecondsPerMinute;** |
|  |  |
|  | **class DioClient {** |
|  | **final String baseUrl;** |
|  |  |

|  |
| --- |
| **Future<dynamic> delete(** |
|  | **String uri, {** |
|  | **data,** |
|  | **Map<String, dynamic> queryParameters,** |
|  | **Options options,** |
|  | **CancelToken cancelToken,** |
|  | **}) async {** |
|  | **try {** |
|  | **var response = await \_dio.delete(** |
|  | **uri,** |
|  | **data: data,** |
|  | **queryParameters: queryParameters,** |
|  | **options: options,** |
|  | **cancelToken: cancelToken,** |
|  | **);** |
|  | **return response.data;** |
|  | **} on FormatException catch (\_) {** |
|  | **throw FormatException("Unable to process the data");** |
|  | **} catch (e) {** |
|  | **throw e;** |
|  | **}** |
|  | **}** |
|  | **}** |

Except the usefulness of the Exception Handling, agency essentially needs to allocate and determine which ports on a network are functioning, open or closed and this can be reached by the process of port scanning (What is port scanning and how does it work? | Avast, 2021). This process of sending packets to specified ports will identify vulnerabilities on our network and managing this flow will deliver security over our systems. It can be produced in the way below:

**# We need to import packages for**

**# the socket,sys,pyfiglet which contains pieces of written code**

**# That allows us to automate certain process**

**import pyfiglet**

**import sys**

**import socket**

**# Exact date and time we need so we know exactly how**

**# Long does it take to execute certain processs**

**from datetime import datetime**

**#We are using the imported before module**

**#And this we will convert text to ASCII art fonts for**

**#Better integrity**

**ascii\_banner = pyfiglet.figlet\_format("PORT SCANNER")**

**print(ascii\_banner)**

**# Defining a target which**

**if len(sys.argv) == 2:**

**# translate hostname to IPv4**

**target = socket.gethostbyname(sys.argv[1])**

**else:**

**print("Invalid amount of Argument")**

**# Add Banner and**

**print("-" \* 50)**

**print("Scanning Target: " + target)**

**print("Scanning started at:" + str(datetime.now()))**

**print("-" \* 50)**

**try:**

**# Will scan ports between 16,656 to 65535**

**for port in range(16656,65535):**

**s = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)**

**socket.setdefaulttimeout(1)**

**# returns an error indicator**

**result = s.connect\_ex((target,port))**

**if result ==0:**

**print("Port {} is open".format(port))**

**s.close()**

**except KeyboardInterrupt:**

**print("\n Exiting Program !”)**

**sys.exit()**

**sys.exit()**

**except socket.error:**

**print("\ Server not responding !")**

**sys.exit()**

Regular penetration testing will be needed to ensure allow system functioning is safe and update, so can deliver the best possible security and test all possible vulnerabilities that can be consist in a software application (Penetration Testing Tutorial: What is PenTest? 2021).Forensic analysis will be needed ,too, so we can learn from the mistakes have been done in the past. Simulating attack can defer to three different types (by employee, network admin or external resource) depending on its scope. In the next example we will see in a script how we can test a Wifi Phisher

|  |
| --- |
|  |
|  |  |
|  | **Import sys**  **try:** |
|  | **raw\_input # Python 2** |
|  | **sys.exit('Please use Python 3 to run Wifiphisher.')** |
|  | **except NameError:** |
|  | **pass # Python 3** |
|  | **#importing needed modules** |
|  | **import logging** |
|  | **import os** |
|  | **#in this case we are going to test the run file of the phisher** |
|  | **from wifiphisher.pywifiphisher import run** |
|  |  |
|  | **root\_logger = logging.getLogger()** |
|  | **root\_logger.addHandler(logging.NullHandler())** |
|  |  |
|  | **dir\_of\_executable = os.path.dirname(\_\_file\_\_)** |
|  | **path\_to\_project\_root = os.path.abspath(os.path.join(dir\_of\_executable, '..'))** |
|  | **sys.path.insert(0, path\_to\_project\_root)** |
|  | **os.chdir(path\_to\_project\_root)** |
|  | **run()** |

The way most of the malware works is attaching to our system or OU (organisational unit) over the internet space ,which will infect ,gain remote access ,steal ,explore ,erase and manipulate anything the attacker wants (Malware | What is Malware & How to Stay Protected from Malware Attacks, 2021).The next example is representing the very popular crypto mining attack with CoinHive(using JavaScript), which will inject certain code and make victim’s machine mining crypto ,without user noticing :



Even though this attack is not as dangerous as the ones before it will still use resources that can lead to a system failure and its also difficult to detect (Ananda Krisha 10/7/2021 ).

By most of this attacks, threats and risks every organisation needs to face nowadays, it needs to stand method, code, script or programme to prevent breaches .But its only a matter of time the expanding and adding new protection techniques to encounter memory and storage issues due to load of all this data . In this case is highly needed using and implementing lazy functional languages and memory management (Wu. J Memory Management in Python 2019) not only because of space but also speed executing well-build efficient Python code will deliver better performance.

Even if we cover all those threats, it will be needed an extra step forward to reduce the biggest, hidden problem in cyber security – Human Factor (cydef.ca 29/10/2021). This can be reached by putting in place a lot of professional training, raise awareness, appropriate access and even social engineering research. In this report we overlooked the most common problems of the cyber and propose techniques and approaches reducing the risk, evaluating the threats and reduce the vulnerabilities

References:

Securitymagazine.com. 2021. *| Security Magazine*. [online] Available at: <https://www.securitymagazine.com/gdpr-policy?url=https%3A%2F%2Fwww.securitymagazine.com%2Farticles%2F96009-the-human-factor-in-cybersecurity>

Kenna Security. 2021. *Risk, Threat, or Vulnerability? What's the Difference | Kenna Security*. [online] Available at: <https://www.kennasecurity.com/blog/risk-vs-threat-vs-vulnerability/>

Hut Six. 2021. *Information Security Principles: What is the CIA Triad?* [online] Available at: <https://www.hutsix.io/information-security-principles-what-is-the-cia-triad/>

Executech. 2021. *Top 15 Types of Cybersecurity Risks & How to Prevent Them | Executech*. [online] Available at: <https://www.executech.com/insight/top-15-types-of-cybersecurity-attacks-how-to-prevent-them/>

Hut Six. 2021. *Information Security Principles: What is the CIA Triad?* [online] Available at: <https://www.hutsix.io/information-security-principles-what-is-the-cia-triad

Nytimes.com. 2021. *A Cyberattack Hobbles Atlanta, and Security Experts Shudder (Published 2018)*. [online] Available at: <https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html>

Lastline. 2021. *Five High-Profile Watering Hole Attacks Highlight Importance of Network Security*. [online] Available at: <https://www.lastline.com/blog/five-high-profile-watering-hole-attacks-highlight-importance-of-network-security/>

BBC News. 2021. *Eurofins Scientific: Cyber-attack leads to backlog of 20,000 forensic samples*. [online] Available at: <https://www.bbc.co.uk/news/uk-49361260#:~:text=Eurofins%20Scientific%20was%20targeted%20by,police%20investigations%20and%20court%20cases.>

Fortinet. 2021. *What Is a Watering Hole Attack? | Fortinet*. [online] Available at: <https://www.fortinet.com/resources/cyberglossary/watering-hole-attack>

Lu Zhou, Mingchao Liao, Cao Yuan, Haoyu Zhang, "Low-Rate DDoS Attack Detection Using Expectation of Packet Size", *Security and Communication Networks*, vol. 2017, Article ID 3691629, 14 pages, 2017.

Learning Center. 2021. *What is a DoS/DDoS Attack Script or Toolkit | DDoS Tools | Imperva*. [online] Available at: <https://www.imperva.com/learn/ddos/ddos-attack-scripts/>

Definitions, E. and Hope, C., 2021. *What is Exception Handling?* [online] Computerhope.com. Available at: <https://www.computerhope.com/jargon/e/exception-handling.htm#:~:text=Exception%20handling%20is%20responding%20to,happens%20that%20requires%20special%20processing.&text=Exception%20handling%20attempts%20to%20gracefully,entire%20system)%20does%20not%20crash.>

GitHub. 2021. *network\_handling/dio\_client.dart at master · ashishrawat2911/network\_handling*. [online] Available at: <https://github.com/ashishrawat2911/network\_handling/blob/master/lib/services/dio\_client.dart>

Avast.com. 2021. *What is port scanning and how does it work? | Avast*. [online] Available at: <https://www.avast.com/en-gb/business/resources/what-is-port-scanning#pc>

Guru99. 2021. *Penetration Testing Tutorial: What is PenTest?* [online] Available at: <https://www.guru99.com/learn-penetration-testing.html>

GitHub. 2021. *wifiphisher/tests at master · wifiphisher/wifiphisher*. [online] Available at: <https://github.com/wifiphisher/wifiphisher/tree/master/tests>

Palo Alto Networks. 2021. *Malware | What is Malware & How to Stay Protected from Malware Attacks*. [online] Available at: <https://www.paloaltonetworks.com/cyberpedia/what-is-malware#:~:text=Malware%20(short%20for%20%E2%80%9Cmalicious%20software,methods%20to%20infect%20computer%20systems.>

Krishna, A. (2018). *How to Detect and Remove Crypto Mining Malware (CoinHive) hack from your WordPress, Magento, Drupal Websites*. [online] www.getastra.com. Available at: <https://www.getastra.com/blog/911/remove-crypto-mining-malware-cms-wordpress-magento-drupal>

Wu, J. (2019). *Memory Management in Python*. [online] Medium. Available at: <https://towardsdatascience.com/memory-management-in-python-6bea0c8aecc9>

CYDEF (2021). *The Human Factor: The Hidden Problem of Cybersecurity*. [online] CYDEF. Available at: https://cydef.ca/blog/the-human-factor-the-hidden-problem-of-cybersecurity/.

‌

‌