Audit of Risk Assessment for Botium Toys

Assets	Value	Associated risk	Likelihood (0-10)	Impact (0-10)	Vulnerability score(0-10)	CVSS	Comment
On-Premises equipment	Critically sensitive	Damage, Misconfiguration,	1	10	5.5	Low	Inadequate management of assets, No proper control in place
Employee Equipment	Medium Sensitive	Lost, Damage, Agent, Insider threat,	8	8	8	High	Inadequate management of assets, No proper control in place
Store products	Medium Sensitive	Damage, Insecurity, Lack of physical access control, Social engineering	5	6	5.5	Low	Inadequate management of assets, No proper control in place
Management System	Critically Sensitive	Injection, Session Hijacking, Information Disclosure, SSRF	9	10	9.9	Critical	Inadequate management of assets, No proper control in place
Internet access	Highly Sensitive	Denial of service, Non-availability, Broken access control, Injection	7	10	8.8	High	Inadequate management of assets, No proper control in place, No full compliant with international regulations and standards
Internal network	Critically Sensitive	Identity and Authentication failure,	10	5	7.5	High	Inadequate management of assets, No proper control in place, No full compliant with international regulations and standards, All Botium Toys employees have access to internally stored data
Data retention and storage	Critically Sensitive	Data loss, Ransomware, Integrity, Confidentiality	8	10	9	Critical	Inadequate management of assets, No proper control in place, No full compliant with international regulations and standards, All Botium Toys employees have access to internally stored data, Encryption is not currently used
Legacy system	Lowly Sensitive	Out of date, incompatibility, Slow	8	2	5	Low	Inadequate management of assets, No proper control in place

File System

File System

Lists of Departments

```
analyst@542a98ef067f:~/Departments$ ls
Finance  HR  Operations  Security  Training
analyst@542a98ef067f:~/Departments$
```

Creating and verifying file1 in the HR Department

```
analyst@542a98ef067f:~/Departments$ touch HR/joseph_file1
analyst@542a98ef067f:~/Departments$ ls HR/
joseph_file1
analyst@542a98ef067f:~/Departments$
```

Creating and verifying file2 in the HR Department

```
analyst@542a98ef067f:~/Departments/HR$ echo "My second way of creating file2" > olusola_file2
analyst@542a98ef067f:~/Departments/HR$ ls
joseph_file1  olusola_file2
analyst@542a98ef067f:~/Departments/HR$
```

Moving and verifying file2 to Training Department and copying to Security Department

```
analyst@542a98ef067f:~/Departments/HR$ ls
joseph_file1  olusola_file2
analyst@542a98ef067f:~/Departments/HR$ mv olusola_file2 ../Training/ && cp ../Training/olusola_file2 ..
/Security/
analyst@542a98ef067f:~/Departments/HR$ ls
joseph_file1
analyst@542a98ef067f:~/Departments/HR$ ls ../Training/ && ls ../Security/
olusola_file2
olusola_file2
analyst@542a98ef067f:~/Departments/HR$
```

Copying and verifying file1 and file2 to other Departments

```
Finance  HR  Operations  Security  Training
analyst@542a98ef067f:~/Departments$ cp HR/joseph_file1 Security/ && cp Security/* Training/ && cp Secur
ity/* Operations/ && cp Security/* Finance/
analyst@542a98ef067f:~/Departments$ tree
.
|-- Finance
|   |-- joseph_file1
|   `-- olusola_file2
|-- HR
|   `-- joseph_file1
|-- Operations
|   |-- joseph_file1
|   `-- olusola_file2
|-- Security
|   |-- joseph_file1
|   `-- olusola_file2
`-- Training
    |-- joseph_file1
    `-- olusola_file2

5 directories, 9 files
analyst@542a98ef067f:~/Departments$
```

INCIDENT REPORT ANALYSIS

SUMMARY	The company experienced a security event when all network services suddenly stopped responding. The Cybersecurity team found the disruption was caused by a distributed denial of services (DDoS) attack through a flood of incoming ICMP packets. The team responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored.
IDENTIFY	The company has assets to protect in order to keep daily business activities from interruption. Assets such as website pages, safety in the internet space, firewalls, public facing web server(s), internal servers as well as social media platforms. We have identified possible threat to these assets which are web page login brute forcing, Denial of Service(DoS)/DDoS as well as account hijacking(social media) among various other threats.
PROTECT	The Cybersecurity team implemented firewall to limit incoming network traffics and an IDS/IPS system to filter out packets based on suspicious characteristics/signatures. Rate limiting has also been configured to prevent brute forcing of user accounts and any other possible attack. Threat awareness training for the company`s staff was organized to get them abreast of possible security threat and social engineering vises.
DETECT	The company's Cybersecurity team then investigated the security even and found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. A malicious actor or actors targeted the company with an ICMP flood attack. The web server is no longer accessible and clients are stranded as daily work flow has been interrupted. The entire internal network was also affected.
RESPOND	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services. A new firewall rule to limit the rate of incoming ICMP packets An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics The Cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns. For future security events, the Cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event.
RECOVER	To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be

	brought back online.

Reflections/Notes:

File Permission and SQL(WEEK 4) Assignment: OLUSOLA Joseph

File Permission and SQL(WEEK 4) Assignment: OLUSOLA Joseph

Checking for file and working directory.

```
analyst@e59259fbf4a6:~$ ls && pwd
/home/analyst
analyst@e59259fbf4a6:~$
```

Creating, confirming and checking permissions for file1 and file2.

```
analyst@e59259fbf4a6:~$ touch file1; echo "" > file2
analyst@e59259fbf4a6:~$ ls
file1  file2
analyst@e59259fbf4a6:~$ ls -l
total 4
-rw-r--r-- 1 analyst research_team 0 Feb 23 10:35 file1
-rw-r--r-- 1 analyst research_team 1 Feb 23 10:35 file2
analyst@e59259fbf4a6:~$
```

Checking, Creating and Verifying user1 account.

```
analyst@22993c91e7b5:~$ tail -n 5 /etc/passwd
messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
student:x:1000:1000::/home/student:/bin/bash
analyst:x:1001:1003::/home/analyst:/bin/sh
researcher2:x:1002:1003::/home/researcher2:/bin/sh
analyst@22993c91e7b5:~$ sudo useradd user1 -p user1passwd
analyst@22993c91e7b5:~$ tail -n 5 /etc/passwd
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
student:x:1000:1000::/home/student:/bin/bash
analyst:x:1001:1003::/home/analyst:/bin/sh
researcher2:x:1002:1003::/home/researcher2:/bin/sh
user1:x:1003:1005::/home/user1:/bin/sh
analyst@22993c91e7b5:~$
```

Checking , Creating and Verifying group1.

```
analyst@22993c91e7b5:~$ tail -n 5 /etc/group
analyst:x:1001:
researcher2:x:1002:
research_team:x:1003:
sales_team:x:1004:
user1:x:1005:
analyst@22993c91e7b5:~$ sudo addgroup group1
Adding group `group1' (GID 1006) ...
Done.
analyst@22993c91e7b5:~$ tail -n 5 /etc/group
researcher2:x:1002:
research_team:x:1003:
sales_team:x:1004:
user1:x:1005:
group1:x:1006:
analyst@22993c91e7b5:~$
```

Since user1 is "other users" in the machine, it already inherited read-only access to file1 by default.

```
analyst@a1643bb6787c:~$ ls -la
total 32
drwxr-xr-x 2 analyst research_team 4096 Feb 23 11:47 .
drwxr-xr-x 1 root    root          4096 Feb 23 11:08 ..
-rw------- 1 analyst research_team  371 Feb 23 12:03 .bash_history
-rw-r--r-- 1 analyst research_team  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 analyst research_team 3597 Feb 23 11:08 .bashrc
-rw-r--r-- 1 analyst research_team 3597 Feb 23 11:08 .profile
-rw-r--r-- 1 analyst research_team    0 Feb 23 11:47 file1
-rw-r--r-- 1 analyst research_team    1 Feb 23 11:47 file2
analyst@a1643bb6787c:~$
```

Verifying Permission, Changing Ownership and Permission of file2, and Reverifying Permission.

```
analyst@8280a548ef0d:~$ ls -la
total 32
drwxr-xr-x 2 analyst research_team 4096 Feb 23 12:17 .
drwxr-xr-x 1 root    root          4096 Feb 23 11:54 ..
-rw------- 1 analyst research_team  354 Feb 23 12:22 .bash_history
-rw-r--r-- 1 analyst research_team  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 analyst research_team 3597 Feb 23 11:54 .bashrc
-rw-r--r-- 1 analyst research_team 3597 Feb 23 11:54 .profile
-rw-r--r-- 1 analyst research_team    0 Feb 23 12:17 file1
-rw-r--r-- 1 analyst research_team    1 Feb 23 12:17 file2
analyst@8280a548ef0d:~$ sudo chown user1 file2; sudo chmod 744 file2; ls -la
total 32
drwxr-xr-x 2 analyst research_team 4096 Feb 23 12:17 .
drwxr-xr-x 1 root    root          4096 Feb 23 11:54 ..
-rw------- 1 analyst research_team  361 Feb 23 12:22 .bash_history
-rw-r--r-- 1 analyst research_team  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 analyst research_team 3597 Feb 23 11:54 .bashrc
-rw-r--r-- 1 analyst research_team 3597 Feb 23 11:54 .profile
-rw-r--r-- 1 analyst research_team    0 Feb 23 12:17 file1
-rwxr--r-- 1 user1   research_team    1 Feb 23 12:17 file2
analyst@8280a548ef0d:~$
```

Verifying group permission, Changing group ownership, and group permission for file1 and file2(group permission for file2 is read-only by default).

```
analyst@8280a548ef0d:~$ ls -la
total 32
drwxr-xr-x 2 analyst research_team 4096 Feb 23 12:17 .
drwxr-xr-x 1 root    root          4096 Feb 23 11:54 ..
-rw------- 1 analyst research_team  420 Feb 23 12:34 .bash_history
-rw-r--r-- 1 analyst research_team  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 analyst research_team 3597 Feb 23 11:54 .bashrc
-rw-r--r-- 1 analyst research_team 3597 Feb 23 11:54 .profile
-rw-r--r-- 1 analyst research_team    0 Feb 23 12:17 file1
-rwxr--r-- 1 user1   research_team    1 Feb 23 12:17 file2
analyst@8280a548ef0d:~$ sudo chgrp group1 file2; sudo chgrp group1 file1; sudo chmod
 674 file1
analyst@8280a548ef0d:~$ ls -la
total 32
drwxr-xr-x 2 analyst research_team 4096 Feb 23 12:17 .
drwxr-xr-x 1 root    root          4096 Feb 23 11:54 ..
-rw------- 1 analyst research_team  498 Feb 23 12:40 .bash_history
-rw-r--r-- 1 analyst research_team  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 analyst research_team 3597 Feb 23 11:54 .bashrc
-rw-r--r-- 1 analyst research_team 3597 Feb 23 11:54 .profile
-rw-rwxr-- 1 analyst group1           0 Feb 23 12:17 file1
-rwxr--r-- 1 user1   group1           1 Feb 23 12:17 file2
analyst@8280a548ef0d:~$
```

SQL

Checking for columns in both machines and employees table

```
MariaDB [organization]> SELECT *
    -> FROM machines
    -> LIMIT 5;
+--------------+------------------+----------------+---------------+-------------+
| device_id    | operating_system | email_client   | OS_patch_date | employee_id |
+--------------+------------------+----------------+---------------+-------------+
| a184b775c707 | OS 1             | Email Client 1 | 2021-09-01    |        1156 |
| a192b174c940 | OS 2             | Email Client 1 | 2021-06-01    |        1052 |
| a305b818c708 | OS 3             | Email Client 2 | 2021-06-01    |        1182 |
| a317b635c465 | OS 1             | Email Client 2 | 2021-03-01    |        1130 |
| a320b137c219 | OS 2             | Email Client 2 | 2021-03-01    |        1000 |
+--------------+------------------+----------------+---------------+-------------+
5 rows in set (0.090 sec)

MariaDB [organization]> SELECT *
    -> FROM employees
    -> LIMIT 5;
+-------------+--------------+----------+-----------------+-------------+
| employee_id | device_id    | username | department      | office      |
+-------------+--------------+----------+-----------------+-------------+
|        1000 | a320b137c219 | elarson  | Marketing       | East-170    |
|        1001 | b239c825d303 | bmoreno  | Marketing       | Central-276 |
|        1002 | c116d593e558 | tshah    | Human Resources | North-434   |
|        1003 | d394e816f943 | sgilmore | Finance         | South-153   |
|        1004 | e218f877g788 | eraab    | Human Resources | South-127   |
+-------------+--------------+----------+-----------------+-------------+
5 rows in set (0.001 sec)

MariaDB [organization]>
```

Full details of the Left Join of Machines and Employees Tables

```
MariaDB [organization]> SELECT * FROM machines LEFT JOIN employees ON machines.employee_id = employees.employee_id LIMIT 10;
+--------------+------------------+----------------+---------------+-------------+-------------+--------------+----------+-----------------------+---------+
| device_id    | operating_system | email_client   | OS_patch_date | employee_id | employee_id | device_id    | username | department            | office  |
+--------------+------------------+----------------+---------------+-------------+-------------+--------------+----------+-----------------------+---------+
| a184b775c707 | OS 1             | Email Client 1 | 2021-09-01    |        1156 |        1156 | a184b775c707 | dellery  | Marketing             | East-417
| a192b174c940 | OS 2             | Email Client 1 | 2021-06-01    |        1052 |        1052 | a192b174c940 | jdarosa  | Marketing             | East-195
| a305b818c708 | OS 3             | Email Client 2 | 2021-06-01    |        1182 |        1182 | a305b818c708 | mmora    | Information Technology | Central-
| a317b635c465 | OS 1             | Email Client 2 | 2021-03-01    |        1130 |        1130 | a317b635c465 | tsnow    | Sales                 | Central-
| a320b137c219 | OS 2             | Email Client 2 | 2021-03-01    |        1000 |        1000 | a320b137c219 | elarson  | Marketing             | East-170
| a398b471c573 | OS 3             | Email Client 2 | 2021-12-01    |           0 |        NULL | NULL         | NULL     | NULL                  | NULL
| a667b270c984 | OS 1             | Email Client 1 | 2021-03-01    |        1078 |        1078 | a667b270c984 | sharley  | Sales                 | North-41
| a821b452c176 | OS 2             | Email Client 2 | 2021-12-01    |        1104 |        1104 | a821b452c176 | mreed    | Information Technology | West-288
| a998b568c863 | OS 3             | Email Client 1 | 2021-12-01    |        1026 |        1026 | a998b568c863 | apatel   | Human Resources       | West-320
| b157c491d493 | OS 2             | Email Client 1 | 2021-03-01    |           0 |        NULL | NULL         | NULL     | NULL                  | NULL
+--------------+------------------+----------------+---------------+-------------+-------------+--------------+----------+-----------------------+---------+
10 rows in set (0.000 sec)
```

OLUSOLA Joseph Pelumi

Risk Assessment for Angels Credit Group (ACG), Abeokuta.

Asset	Threat	Likelihood	Impact	Priority	Justification	Recommendation
Customer record	Unauthorized access	3	3	9	Unauthorized access is the entry point to all endpoints/hosts or networks. This could be achieved when the organization is not enforcing strong password policy, lacking awareness against phishing attack, presence of insider threat, stolen credentials, no adequate access control in place, lack of physical security control, non enforcement of strong encryption. One or all of these put customers records/accounts to free for all.	Encryption of data (at-rest and in-transit)should be introduced. The principle of least privilege and need to know should be applied. Strong access authentication method should be put in place and the policy of secure password be enforced. Proper configuration of application software and hosts to prevent XSS, SSRF among other attacks. Enforcing rate limiting to mitigate against password bruteforcing is also a good idea.
Local web server	Unavailability of server	3	1	3	This could result from system update and upgrade or some other maintenance. Other cause may be application failure or bug that may make the application server behave in an unexpected manner. Excess traffic request or DOS may also be a cause.	Creation of alternative server to help in sharing of high traffic using load ballancer. Provision of backup server to fallback to in case of failure of a single server. Installation of IDS/IPS to prevent the instance of DOS/DDOS, by filtering multiple requests from identified(rouge) IP.
Company laptop	Malware	1	3	3	User behaviour, security practices and endpoint security are determinant of possible malware infection. As it contributes to data loss, financial impact, intellectual property and network propagation.	Implementation of security policies such as USB security policy, patch management, incident response plan, mobile device management, backup and recovery plan, network security measures, access controls, employee training, regular software updates and endpoint security software among others will secure the company's laptop from malware threats.
Employees laptop	Compromised customers' and company's	1	3	3	Bring Your Own Devices(BYOD) policies has its associated risks such as data leakage, malware threats and	Organization must establish clear security guidelines, enforce strong authentication, implement Mobile Device

Risk Assessment for Angels Credit Group (ACG), Abeokuta.

	data				device theft among others. Insufficient update management, regulatory compliance and compatibility issues as well as privacy concern are issues to contend with.	Management(MDM) solutions and educate employees. Regular security updates, audits and monitoring can also help to mitigate potential risks.
Employees records	Social Engineering	3	3	9	If the identity or information of employees are publicly available, threat actors could take the advantage, performing social engineering within the organization's employees. In case where attacker have access to employees names, location, official mail and the rest, attacker can perform identity theft, fraud, phishing, corporate espionage and business disruption.	Employees record and details must be placed with high priority as their official identity must be secretive. Personal information should not be mixed with official information, i. e. personal mail should be used for official transactions Regular training must me given to employees to identify social engineering devices. Proper incident response plan be put in place against such occurrences, as well as regular audits and monitoring, compliance and regulations.
Business records & information	Data Breach	1	3	3	Unauthorized access, malware, possibility to compromise customers' or/and company's data, social engineering to mention but a few are all indication to data breaches. This is an unauthorized access to business records, exposing sensitive information and reputation damage which could lead to business collapse that may also include fines.	Strong encryption method to protect sensitive business records, strict access control and users' authentication mechanism, regular data backup, employees training, robust security endpoint solution, regular test of incident response plan, implementation of IDS/IPS to prevent network, data classification based on sensitivity, as well as employee awareness are all needed to mitigate against this form of attack/threat.

OLUSOLA, Joseph Oluwapelumi

Incident handler's journal

Date: March 10, 2024	Emotet.exe
Description	Analyzing Emotet.exe for Possible Malicious Activities
Tool(s) used	Wireshark
The 5 W's	● **Who**: A process named Emotet.exe was running as root ● **What**: This was discovered to be a Banking Trojan ● **Where**: This incident occurred in one of TedprimeHub's outlet machine ● **When**: Between the hours of 2:00Hr and 5:00Hr GMT+1 ● **Why**: This attack must have been due to a discovered server misconfiguration. After a successful infiltration, a Command and Control (C2) server with the IP Address of 10.1.6.206 was ex-filtrating company's sensitive data through a compromised public server with the IP Address of 87.252.164.58, which then further exposed the internal network including IP Addresses 66.153.205.191, 173.255.195.246, 103.92.235.25 and 5.2.136.39 communicating with the C2 server.
Additional notes	1. Proper reconfiguration of server and host be made, and patches be updated. 2. Firewall, IDS/IPS, with Anti-Virus be given priority. 3. Proper network monitoring should be up-scaled.