ABC Company
Threat Identification, Analysis and Risk Assessment (TIARA) Report (March 2020)

Make IT Simpler, More Secure and Valuable

Sangfor Technologies
Block A1, Nanshan iPark, No.1001 Xueyuan Road,Nanshan District, Shenzhen, China
T.: +60 12711 7129 (7511) | E.: sales@sangfor.com | W.: www.sangfor.com

Document Details

Name	ABC Company Threat Identification, Analysis and Risk Assessment (TIARA) Report (March 2020)		
Version	V1.0		
ID	SFSS-VS-R0101		
Author	Jeffrey Lee	**Issue Date**	14 March 2020
Reviewed By	Sangfor MSS Team	**Review Date**	14 March 2020
Classification	Confidential		
Limited To	• Sangfor Technologies Inc. • ABC Company		
Distribution Control	Sangfor Technologies Inc.: CREATE, MODIFY, READ	ABC Company: READ	

Version Change Record

Modified Date	Version	Description	Modified By
14 March 2020	V1.0	Final Draft	Jeffrey Lee

Disclaimer

This document contains Sangfor Technologies confidential commercial information. By accepting the terms, you agree to keep this document strictly confidential, and not reproduce, transmit or disclose any or all of this document to any person or entity, without prior written permission from Sangfor. If you do not wish to accept the terms, note that disclosure, reproduction and transmission of any or all of this document, in any form, will result in litigation.

Table of Contents

1. General Description 4

2. Objectives 4

3. Executive Summary 5

4. Activity Details 7

4.1 Assessment Date 7
4.2 Field Engineer 7
4.3 Security Consultant 7

5. Risk Level 8

6. Assessment Summary 9

6.1 Summary of Threats Identified 9
6.2 Business Impact Analysis 10
6.3 Compliance Impact Analysis 12
6.4 Gap Analysis 12

7. Hardware Components Health Check Result 14

7.1 Policy and Configuration Check 15

8. Security Events and Threats Analysis 17

8.3 Outdated Software with Known Vulnerabilities 17
8.4 Attack Behaviors 20
8.5 Suspicious Behaviors 22

9. Long-Term Recommendations 27

1. General Description

In order to ensure the overall security of the system within ABC Company (ABC), ensure the confidentiality, integrity and availability of the system, and ensure network security is effectively protected, Sangfor Technologies Inc. was commissioned to conduct a Threat Identification, Analysis and Risk Assessment (TIARA) service, with the aid of Cyber Command components, with the goal of identifying any security vulnerabilities and threats currently existing on the network. The TIARA is a preliminary lightweight security posture assessment service which not only could help customers in determine their current threat posture in short period of time, but provide recommendations, improvement plans and remediation assistance in improving security posture into next level.

ABC bears the responsibility of effectively preventing the occurrence of real security incidents, due to the risks and threats discovered during the TIARA service.

2. Objectives

Through Threat Identification, Analysis and Risk Assessment (TIARA) service, the following objectives will be achieved:

- To identify various attack surfaces, threats and weaknesses that could bring adverse effects and impact to the organization
- To identify whether the current security measures of the organization are implemented properly and are still effective in the ongoing operations of the organization
- To uncover hidden malwares within the organization networks and to determine the attack path, kill chain and entry points on how the malwares came into internal network
- To identify if there are any unacceptable risks in the organizational systems
- To identify the gap between current implementation and minimum industry best practice recommendations

3. Executive Summary

Attack	Suspicious Behavior	Vulnerability
Count: **1**	Count: **2**	Count: **2**

ABC Company is a company that offers online transaction platform to its client and end users. As this online transaction platform is the online payment gateway that need to process a lot of sensitive information, such as Personal Identifiable Information (PII) that includes credit card number, cardholder name, address and other information. TIARA assessment to ABC Company should be considered from Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR) and Personal Data Protection Act (PDPA) perspective.

There were total 5 events detected during the assessment period. Out of these 5 events, 1 of them belongs to attack category, 2 of them were related to abnormal behaviors, while 2 of them were related to vulnerabilities. Two of the abnormal behaviors (internal scanning and shared root drive) may be genuine activity that done by internal employee or system administrator. Although this behavior may not seems to be in line with industry best practice or company policy, the system administrator may perform this kind of activities due to business needs. This would require confirmation by ABC Company. The remaining one abnormal behavior would be bruteforce attack detected from internal PC to Internet. This may be conducted by malicious internal actor, or the PC was controlled by remote attacker, or the PC was installed with malicious software that could run processes in the background. This require thorough review by ABC as well.

Furthermore, it was noticed that there were two web servers were hosting and running outdated software version. Although these two web servers are not categorized under host in assessment scope, however the flaws exists on these servers may cause certain risks and impacts to the protected network range too. Should the vulnerabilities being exploited, this will bring risk to whole organization network.

It was noted that there's **insufficient VLAN segregation** practice in the ABC's organization, this will weaken the purpose of VLAN segregation where only allow athorized traffics to pass through. Not only that, ABC does not use **static IP address** on each host, instead using DHCP. This is good in terms of user experience and workload as system administrator do not need to configure IP address for each host, however this could increase the difficulty of tracebility in case a security incident happens. This is because system administrator unable to locate the infected machine due to the dynamic behavior of IP address. It is recommended that VLAN segregation is implemented properly and static IP address is enforced.

4. Activity Details

4.1 Assessment Date

The assessment was performed at the following time, as agreed:

Onsite Period			
Start Date	26-2-2020	**End Date**	26-2-2020

Internal Threat Assessment Period			
Start Date	26-2-2020	**End Date**	4-3-2020

4.2 Field Engineer

Project field engineer details are as follows:

Name		XXXX
Contact	**Phone**	XXXX
	Email	XXXX
Qualification		XXXX

4.3 Security Consultant

Project security consultant details are as follows:

Name		XXXX
Contact	**Phone**	XXXX
	Email	XXXX
Qualification		CREST Registered Tester (CRT), Offensive Security Certified Professional (OSCP), CompTIA Pentest+, Certified Ethical Hacker (CEH)

5. Risk Level

Level	Description
High / Impacted	The event that categorized under this categorized indicates that: • Critical hardware policy not properly configured • High-risk event that potentially / already impacted the host It indicates that the organization not only do not have reasonable level of security protection mechanisms that protecting the network and endpoints of the organization, but do not have sufficient standard operation procedures which in line with industry best practices as well. Should a high-risk attack is successful, it could bring very high level of damages and impacts to the organization.
Medium / Warning	The event that categorized under this categorized indicates that: • Important hardware policy not properly configured • medium-risk event that potentially / already impacted the host It indicates that the organization may have reasonable level of security protection mechanisms that protecting the network and endpoints of the organization. However, due to insufficient standard operation procedures which not in line with industry best practices, the organization may still have certain vulnerabilities and risks that could used and exploited by multiple attacks.
Safe / Not Impacted	The event that categorized under this categorized indicates that: • Policy are properly configured • Events that had been blocked and do not have impact ot the host The organization that falls under this category not only have sufficient level of security protection mechanism, that protecting the network and endpoints of the organization, but it follow most standard operation procedures which in line with industry best practices as well.

6. Assessment Summary

A summary of status results is shown in the tables below. Please see section 6 and 7 for details of each issues detected.

6.1 Summary of Threats Identified

No	Threats Name	Affected Hosts	Status
1	Outdated Software with Known Vulnerabilities	192.168.55.79 192.168.55.110	Warning
2	Attack Behaviors	192.168.46.98	Impacted
3	Suspicious Behaviors	192.168.45.5 192.168.45.7 192.168.45.11 192.168.46.10 192.168.46.46	Impacted

6.2 Business Impact Analysis

6.2.1 Business Impact Matrix

The table below shows the business impact matrix on the assessment of impact on the business operation against the urgency of when the organization should take actions on remediate the issue.

		Impact		
		Significant / Large Affecting Business Unit, Department	**Moderate / Limited** Multiple Users	**Minor / Localized** Single Users
Urgency	**High** No longer able to provide business operation as normal	High	High	Medium
	Medium Work function impaired, but still able to provide part of the business operation	High	Medium	Low
	Low Business operate as normal, but cause inconvenience to certain group of people	Medium	Low	Low

6.2.2 Business Impact Analysis

No	Affected System	Impact	Status
1	eBanking Platform Server	Should the vulnerabilities being exploited, an attacker could execute remote arbitrary code on the server and compromise the server. Once the attacker take control on the server, he or she could introduce trojan, malware or ransomware into the compromised server. Once the ransomware being executed, all the data and files in the serve would be encrypted and this will cause the business operation down.	High
2	eBanking Platform Server	One of the application Content Managmenet System (CMS) in eBanking platform server was using plaint text protocol as login page. This will allow Man-in-The-Middle attack where the content may be edited by malicious actor and sensitive information may be captured. This has greatly violate two elements from CIA triad – Confidentiality and Integrity.	High
3	Log Server	The log server seems to be affected by malware. The malware installed on the log server continuously sending multiple DNS requests to an external server. The victim server may detect these request traffics as DDOS traffic and may make a complain to the ABC via ISP. In this case, the image and reputation of ABC may be affected.	Low

6.3 Compliance Impact Analysis

No	Affected System	Compliance Standard	Analysis	Status
1	eBanking Platform	PCI DSS	There's no VLAN segregation between the eBanking platform system and other internal systems. In this case, an attacker who had compromised one of the internal servers could attack this eBanking Platform server.	Incompliance
2	eBanking Platform	PCI DSS	It was noted that there's improper ruleset configuration on the firewall that protecting the eBanking Platform.	Incompliance

6.4 Gap Analysis

No	Current Situation	Expected Situation	Mitigation Period
1	Lack of VLAN segregation	Implement VLAN segregation to ensure only authorized traffics to go through.	3 months
2	Improper firewall ruleset policy configuration	To review the firewall ruleset policy and ensure only allow authorized traffics from source to destination.	3 months
		To implement internal policy, change management and ensure review every ruleset before make any changes (add, delete, modify) to the firewalls.	1 month
3	Lack of network visibility	To implement network analysis tool to identify hidden threats, hidden	6 months

No	Current Situation	Expected Situation	Mitigation Period
		malware and bypassed attack traffics.	

7. Hardware Components Health Check Result

This section checks the following information of each hardware components, in order to ensure these information meet minimum security requirement and able to continue to support business operation with maximum capabilities:

- Operating Status
- Policies
- Configurations
- Rule Bases Status
- Serial Number

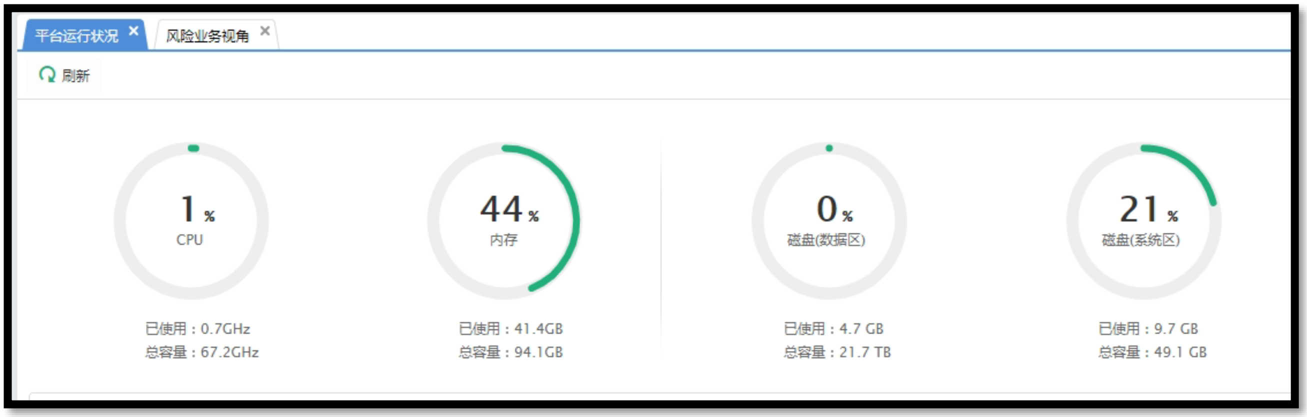
The integrated hardware components information as below:

No	Hardware Type	Account	Status	IP Address	Hardware Hostname	Physical Location
1	Cyber Command (Version: SIP3.0.42.0)	Admin	Online	192.168.45.200	XXXXX	XXXXX
2	STA (Version: STA3.0.17.1878)	Admin	Online	192.168.45.2	XXXXX	XXXXX

7.1 Policy and Configuration Check

7.1.1 Cyber Command Operating Status Check

All components were under online and good performance status	**Status**	Safe

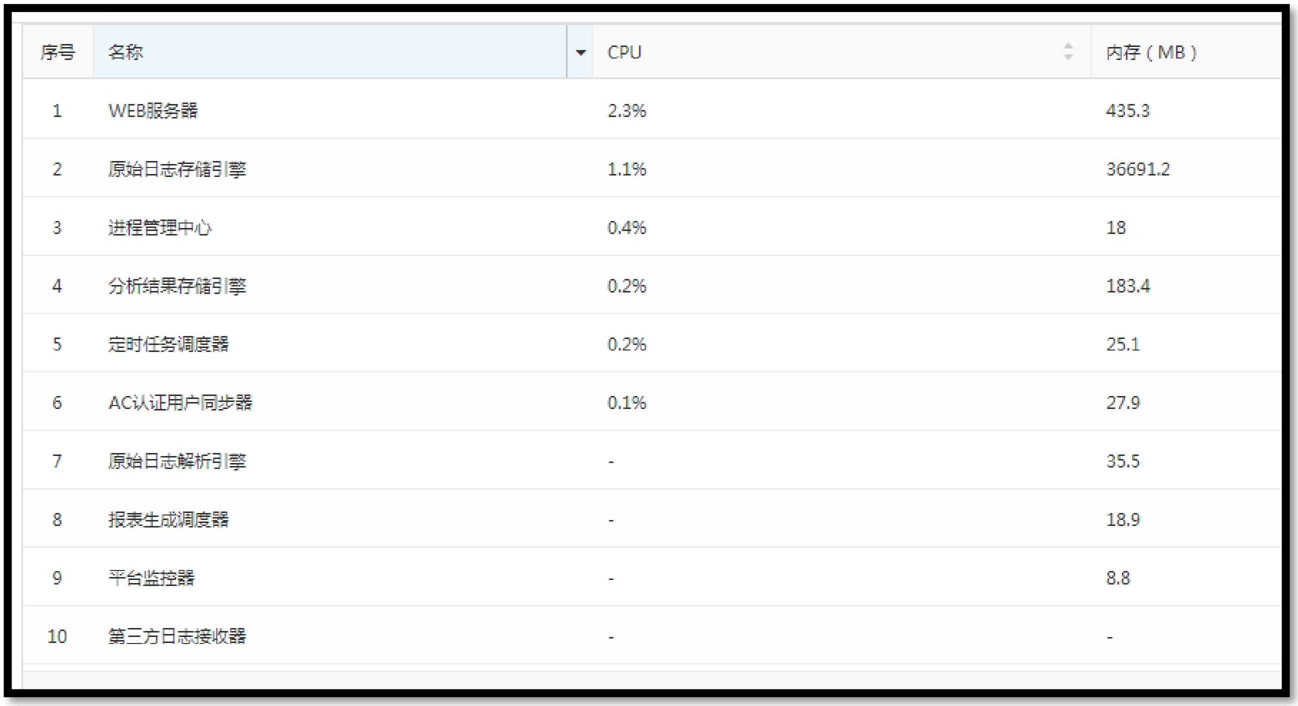


1 % CPU
已使用：0.7GHz
总容量：67.2GHz

44 % 内存
已使用：41.4GB
总容量：94.1GB

0 % 磁盘(数据区)
已使用：4.7 GB
总容量：21.7 TB

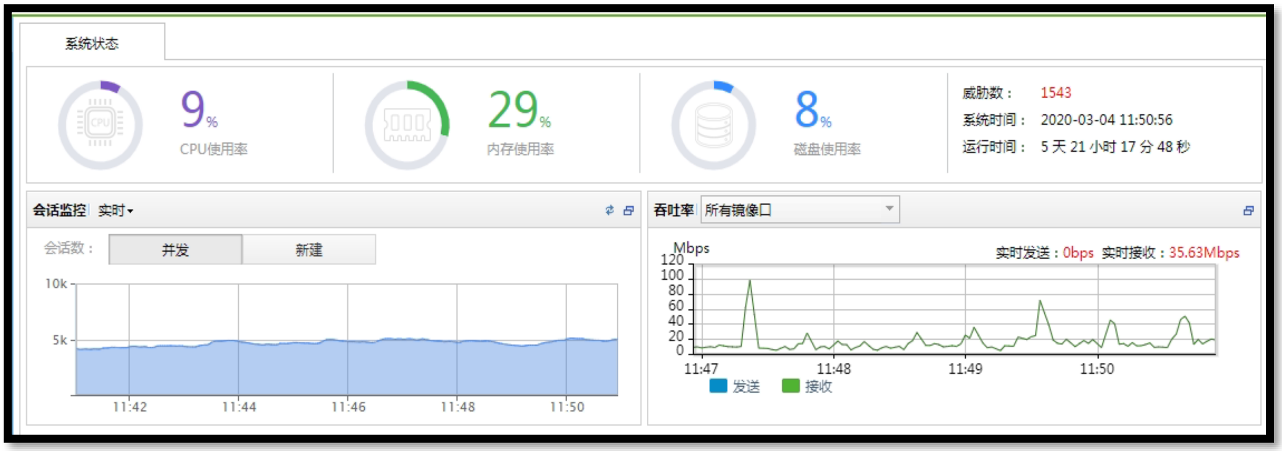
21 % 磁盘(系统区)
已使用：9.7 GB
总容量：49.1 GB



序号	名称	CPU	内存（MB）
1	WEB服务器	2.3%	435.3
2	原始日志存储引擎	1.1%	36691.2
3	进程管理中心	0.4%	18
4	分析结果存储引擎	0.2%	183.4
5	定时任务调度器	0.2%	25.1
6	AC认证用户同步器	0.1%	27.9
7	原始日志解析引擎	-	35.5
8	报表生成调度器	-	18.9
9	平台监控器	-	8.8
10	第三方日志接收器	-	-

Recommendation	N/A

7.1.2 STA Operating Status heck

<table>
<tr><td>All components were under online and good performance status</td><td><b>Status</b></td><td>Safe</td></tr>
<tr><td colspan="3">
系统状态
9%
CPU使用率
29%
内存使用率
8%
磁盘使用率
会话监控
实时
会话数：
并发
新建
10k
5k
11:42
11:44
11:46
11:48
11:50
吞吐率
所有镜像口
Mbps
120
100
80
60
40
20
0
11:47
11:48
11:49
11:50
🟦 发送
🟩 接收

威胁数： 1543
系统时间： 2020-03-04 11:50:56
运行时间： 5 天 21 小时 17 分 48 秒
实时发送：0bps 实时接收：35.63Mbps</td></tr>
<tr><td><b>Recommendation</b></td><td colspan="2">N/A</td></tr>
</table>

8. Security Events and Threats Analysis

Security events and threats analysis are mainly refers to the analysis of centralized management of logs, collection and summarizing of logs of the hosts in scope. Security events and logs analysis play an important role in daily security operations. The purpose of the analysis is to discover threats and risks in the internal network in advance, and fix them as soon as possible, before these threats and risks outbreak and turn into real security incidents.

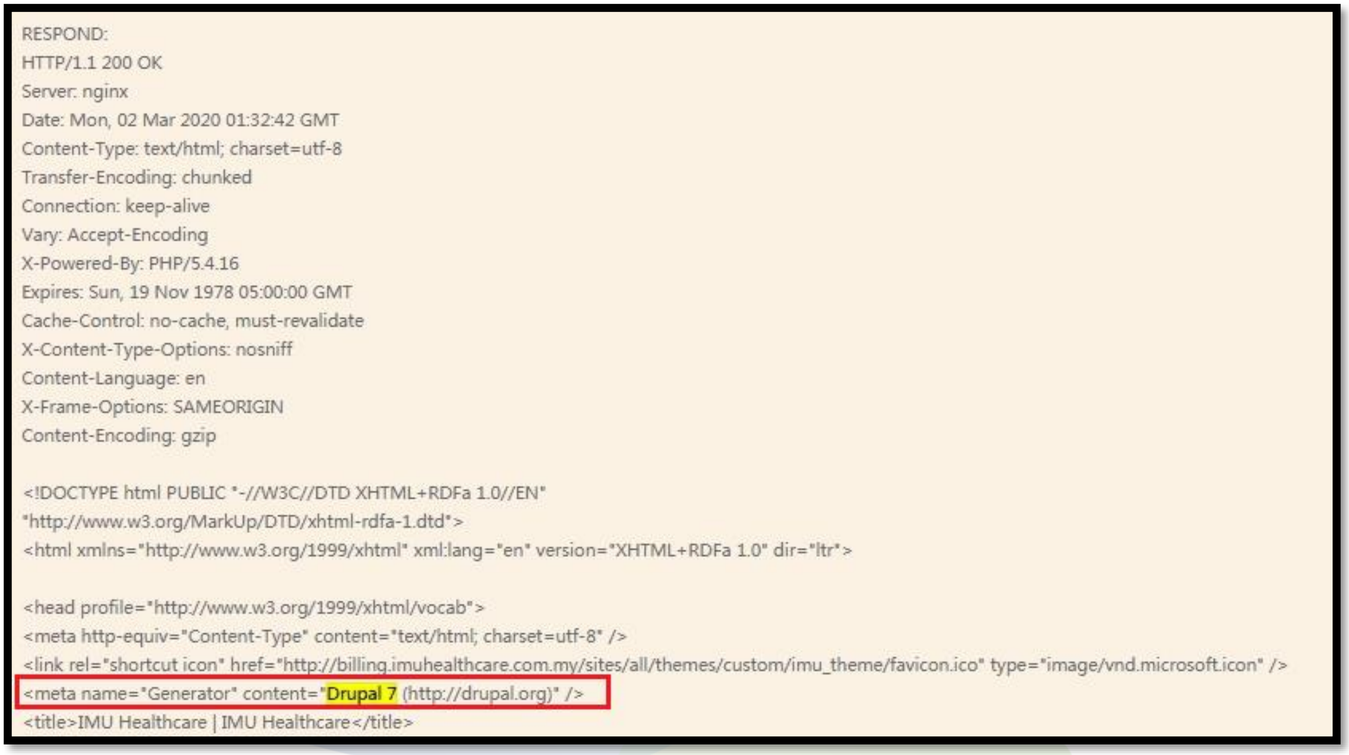
8.3 Outdated Software with Known Vulnerabilities

It was observed that two of the web servers, 192.168.55.79 and 192.168.55.110, are hosting a web application on port TCP/80. Although this it does not belongs to the assets in scope for monitoring, which is 192.168.45.0/24 and 192,.168.46.0/24, it will bring certain impacts to these environments should the vulnerabilities being exploited.

8.3.1 Outdated Drupal Version

It was observed that one of the web server, 192.168.55.79, is running outdated Drupal Content Management System (CMS) version. This outdated Drupal, version 7, is known to be vulnerable to Denial of Service (DoS) attack. In current version, the _filter_url function in the text filtering system (modules / filter / filter.module) have insufficient secure coding practice, and thus has a complex algorithm vulnerability. This could allow a remote attacker to induce a Denial of Service (DoS) condition with long email addresses.

No	Source IP Address	Port	Software	Version
1	192.168.55.79	TCP/80	Drupal	7



```
RESPOND:
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 02 Mar 2020 01:32:42 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.16
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: en
X-Frame-Options: SAMEORIGIN
Content-Encoding: gzip

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML+RDFa 1.0//EN"
"http://www.w3.org/MarkUp/DTD/xhtml-rdfa-1.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" version="XHTML+RDFa 1.0" dir="ltr">

<head profile="http://www.w3.org/1999/xhtml/vocab">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="shortcut icon" href="http://billing.imuhealthcare.com.my/sites/all/themes/custom/imu_theme/favicon.ico" type="image/vnd.microsoft.icon" />
<meta name="Generator" content="Drupal 7 (http://drupal.org)" />
<title>IMU Healthcare | IMU Healthcare</title>
```

Version Disclosure from HTTP Page Source

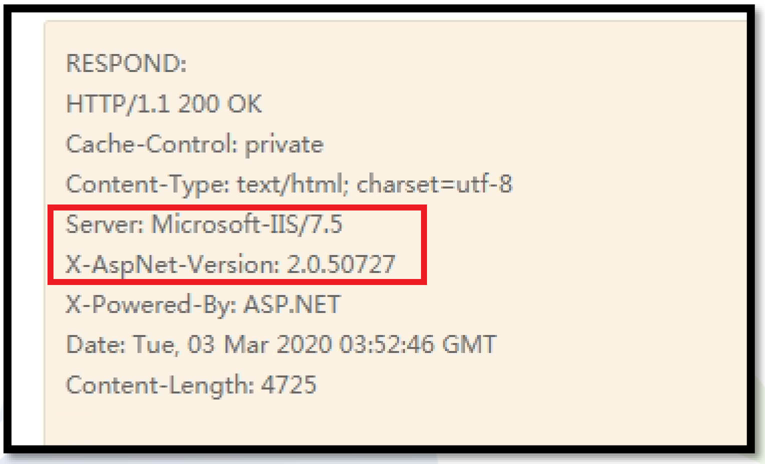
Solution Proposals:

- Ensure conduct penetration testing activity before migrating the web application to production environment
- Ensure update software security patch in a regular basis
- Recommend to disable port TCP/80 and enable port TCP/443 (with SSL) in order to prevent Man-in-The-Middle (MiTM) attack

8.3.2 Outdated Microsoft IIS Version

It was observed that one of the web server, 192.168.55.110, is running outdated Microsoft IIS version. This outdated Microsoft IIS version, 7.5, is known to be vulnerable to buffer overflow attack. There is a buffer overflow in TELNET_STREAM_CONTEXT::OnSendData function of ftpsvc.dll in FTP service. This vulnerability allows an attacker to execute remote arbitrary code via a specially crafted FTP command or cause a Denial Of Service (DOS).

No	Source IP Address	Port	Software	Version
1	192.168.55.110	TCP/80	Microsoft IIS	7.5



```
RESPOND:
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
Date: Tue, 03 Mar 2020 03:52:46 GMT
Content-Length: 4725
```

Version Disclosure From HTTP Response Header

Solution Proposals:

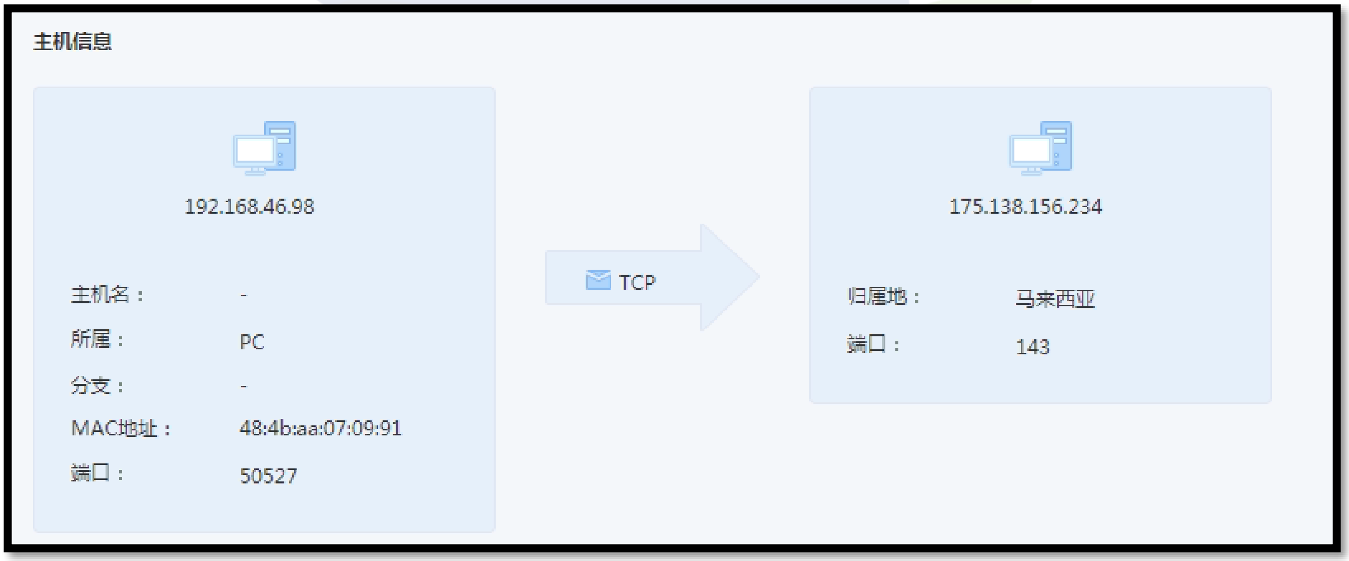
- Ensure conduct penetration testing activity before migrating the web application to production environment
- Ensure update software security patch in a regular basis
- Recommend to disable port TCP/80 and enable port TCP/443 (with SSL) in order to prevent Man-in-The-Middle (MiTM) attack

8.4 Attack Behaviors

8.4.1 IMAP Bruteforce Attack

It was observed that one of the PCs in the network was trying to gain access to IMAP service via bruteforce attack.

No	Source IP Address	Username	Destination IP Address	Port	Count per Minute	Date Time Detected
1	192.168.46.98 (48:4b:aa:07:09:91)	XXXX	175.138.156.234	TCP/143	140	03-03-2020 17:48:39
2	192.168.46.98 (48:4b:aa:07:09:91)	XXXX	175.138.156.234	TCP/143	384	03-03-2020 15:22:14
3	192.168.46.98 (48:4b:aa:07:09:91)	XXXX	175.138.156.234	TCP/143	185	03-03-2020 14:52:13
4	192.168.46.98 (48:4b:aa:07:09:91)	XXXX	175.138.156.234	TCP/143	18	03-03-2020 14:40:35
5	192.168.46.98 (48:4b:aa:07:09:91)	XXXX	175.138.156.234	TCP/143	32	03-03-2020 14:19:48



主机信息

192.168.46.98

主机名： -
所属： PC
分支： -
MAC地址： 48:4b:aa:07:09:91
端口： 50527

175.138.156.234

归属地： 马来西亚
端口： 143

Attack Packet Detected

Bruteforce activity is a common activity for a malicious attacker to obtain the username and password, then gain access to the targeted services. Once attacker successfully gained access to the targeted services, the attacker could have certain controls on that service. By perform enumeration and exploit existing vulnerabilities, the attacker could possible escalate the privilege to administrator rights. Once attacker have administrator's privilege of the targeted service, there's high chance for attacker to compromise the hosted machine and continue to attack other hosts in the environment.

The hosts detected are likely to be controlled by an external attacker to behave like a zombie machine or jumping machine in an attempt to control more hosts on the intranet; or there may be an internal malicious user behavior in the intranet. The risk of this machine being compromised by malicious hackers as follow:

- Theft of confidential information, some confidential documents, usernames and passwords of key assets, etc..
- The host as a zombie machine, will attack other units in both internet and intranet network, and this is violate the local network security law and may possibly penaltied by local regulatory bodies.

Solution Proposals:

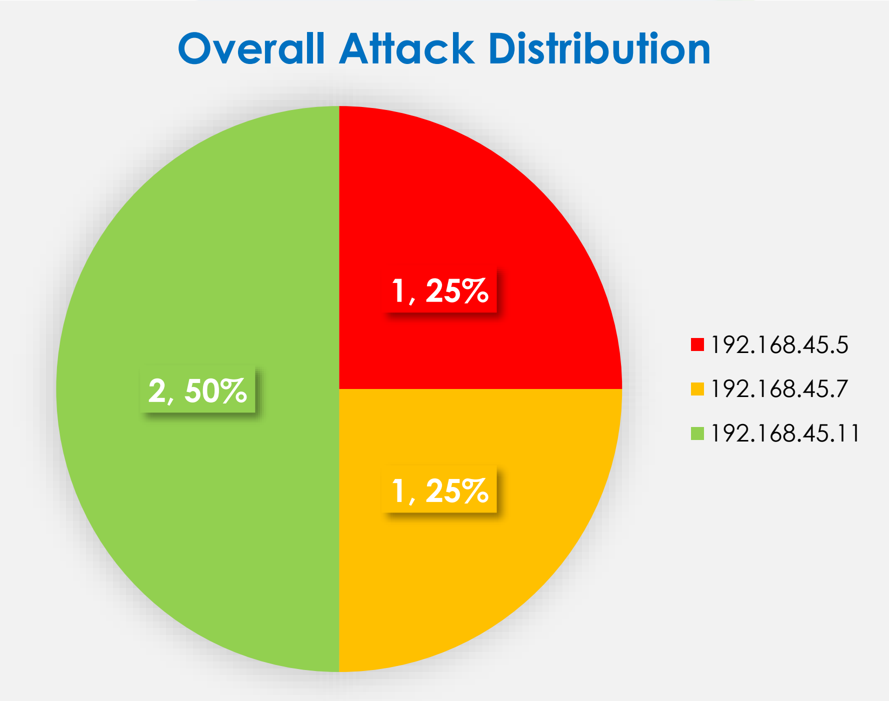
- Ensure restrict only necessary software installed on every host
- Confirm if the behaviors were operated by internal employees, and if so, recommend to train and guide internal employees in accordance with the internal rules and regulations of the organization
- Avoid use of DHCP IP address for security incident tracebility purpose
- Perform firewall ruleset review or implement internet access manager and ensure only allow authorized traffics to Internet

8.5 Suspicious Behaviors

This type of events usually refers to a vulnerability exploitation behavior, malware installation, east-west attacks that may have a strong destructive effect on the system and the application.

8.5.1 Default Share Behavior

It was observed that there were 4 events were related to this default share suspicious behavior activities. There were traffics observed that initiated from 192.168.45.5 (consists of 25%), 192.168.45.7 (consists of 25%) and 192.168.45.11 (consists of 50%).

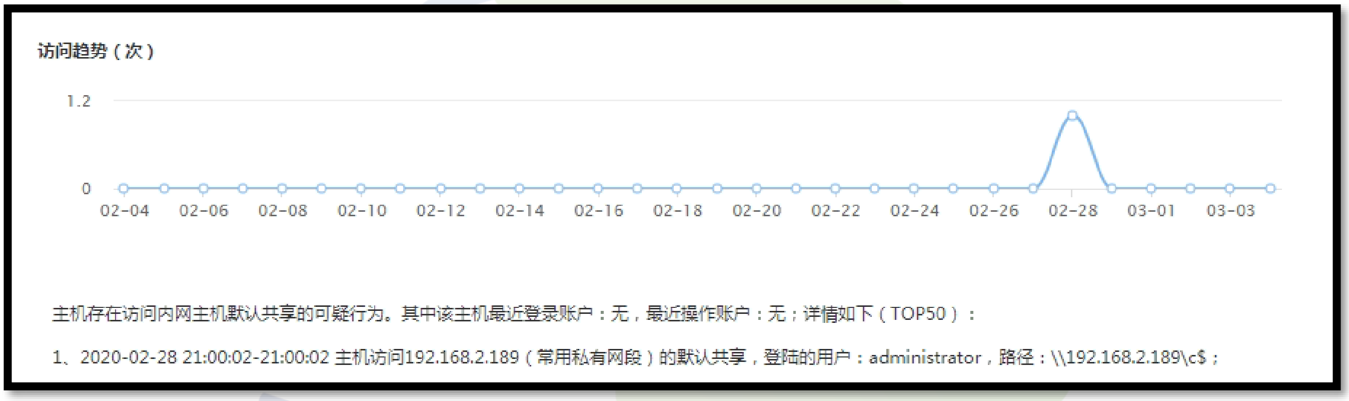


Overall Attack Distribution of Default Share Behavior

It was observed that these three source IP addresses were accessed to C drive of host with IP address **192.168.2.189**.

The following table contains the IP addresses that accessed the shared C drive:

No	Source IP Address	Destination IP Address	Count	Drive	Username Used	Date Time Detected
1	192.168.45.5	192.168.2.189	1	C:\	Administrator	2020-02-28 20:39:00
2	192.168.45.7	192.168.2.189	1	C:\	Administrator	2020-02-28 21:00:02
3	192.168.45.11	192.168.2.189	2	C:\	Administrator	2020-02-28 20:45:28 2020-02-27 13:27:47



主机存在访问内网主机默认共享的可疑行为。其中该主机最近登录账户：无，最近操作账户：无；详情如下（TOP50）：

1、2020-02-28 21:00:02-21:00:02 主机访问192.168.2.189（常用私有网段）的默认共享，登陆的用户：administrator，路径：\\192.168.2.189\c$；

Share Drive Traffic and Command Detected

In Windows system, user can always share the directories, drives and partitions to other machines for the convenience of administrator in managing the servers. However, this is actually a security vulnerabilities in the internal network. Internal user with malicious intentions or external attacker with access to one of the internal machines can always exploit on this feature to perform further post-exploitation activities, These attackers could upload malicious files through the default share, and then can create malicious services or scheduled tasks to execute malicious code, thereby endangering system security and compromising the entire organization's network.

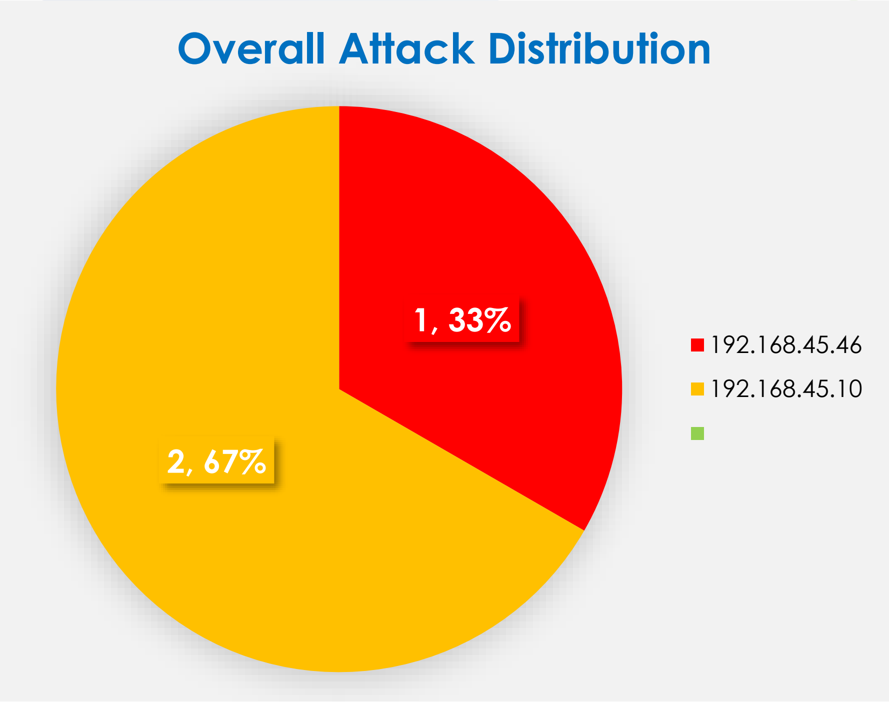
Solution Proposals:

- Ensure disable default share of all hosts from Active Directory policy and only allow the default share on necessary machines
- If share drive is necessary, recommend to share only certain folders, instead of C root drive

- Change administrator password with strong password complexity and only allow authorized personnel to have administrator password
- Confirm if the default share is required for business needs; if so, include the host IP address to global whitelist policy
- Confirm if the behaviors were operated by internal employees, and if so, recommend to train and guide internal employees in accordance with the internal rules and regulations of the organization;
- Ensure apply latest Microsoft security patches on all hosts

8.5.2 Internal Scanning Behavior

It was observed that there were 3 events were related to this internal scanning suspicious behavior activities. There were traffics observed that initiated from 192.168.46.46 (consists of 33%) and 192.168.45.10 (consists of 67%).



Overall Attack Distribution of Internal Scanning Behavior

It was observed that these two source IP addresses were performed scanning activity on random IP addresses via multiple ports.

The following table contains the IP addresses that performed internal scanning:

No	Source IP Address	Username	Destination IP Address Ranges	Date Time Detected	Remarks
1	192.168.46.10	NorShahirah	172.22.1.0/24 172.22.3.0/24 192.168.2.0/24 192.168.4.0/24	03-03-2020 12:41:51	Number of Scan Failures: 886 times Total Number of Scan IPs: 793
			192.168.45.0/24 192.168.55.0/24	27-02-2020 19:05:07	Number of Scan Failures: 518 times Total Number of Scan IPs: 539
2	192.168.46.46	eevon_choy		28-02-2020 18:08:00	Number of Scan Failures: 219 times Total Number of Scan IPs: 222

Scanning is a common pre-activity for a malicious attacker to start to attack and threatens users' networks. The hosts were performed IP scanning on other hosts in order to locate live hosts, and then performs port scanning on these live hosts in order to find the weaknesses of the intranet hosts. Should a vulnerability discovered during the scanning, the attackers could exploit the vulnerability and gain access and comprise this host, and then continue to scan, exploit and compromise other hosts in other segments.

The hosts detected are likely to be controlled by an external attacker to behave like a zombie machine or jumping machine in an attempt to control more hosts on the intranet; or there may be an internal malicious user behavior in the intranet. The risk of this machine being compromised by malicious hackers as follow:

- Theft of confidential information, some confidential documents, usernames and passwords of key assets, etc..

- The host as a zombie machine, will attack other units in both internet and intranet network, and this is violate the local network security law and may possibly penaltied by local regulatory bodies.

Solution Proposals:

- Ensure restrict only necessary software installed on every host
- Confirm if the scanning is required for business needs, such as in house vulnerability scanning activity; if so, include the host IP address to global whitelist policy
- Confirm if the behaviors were operated by internal employees, and if so, recommend to train and guide internal employees in accordance with the internal rules and regulations of the organization;
- Ensure apply latest Microsoft security patches on all hosts
- Suggest to perform VLAN segregation on server and user segments and only allow necessary traffics to pass through

9. Long-Term Recommendations

As network security is a process of dynamic change, to ensure continuous protection of the organization, ABC Company (ABC) should:

1. Strengthen over-all security prior to migrating any host or devices into a production environment
2. Review the operation of each host and application, and backup system data and system logs on a regular basis
3. Conduct security assessment and monitor the security status of the network regularly, documenting all findings for audit purpose as well
4. Ensure security patches for both software application and operating system are apply in a regular basis
5. Ensure the policies of network security equipments are hardened and properly implemented
6. Ensure Active Directory policies are reviewed regularly to ensure all settings are properly enforced
7. Communicate regularly with Sangfor and with key stake-holders in the organisation

Remarks:

In order to prevent data loss due to human or technological error, please ensure all important data is backed-up prior to performing any vulnerability patching or security hardening. It is recommended that the host be restarted after applying the fixes.