សាអលឌិន្យាល័យអូមិនួនីតិសាស្ត្រ និចឌិន្យាសាស្ត្រសេដ្ឋភិច្ច



សារឈាមញ្ចម់ភារសិត្យា

# ភារភារបារនិត្តន័យអូនប្រើប្រាស់ ត្ភូខប្រព័ន្ធណែតទ៉ីន

ស្រាវជ្រាវពីថ្ងៃទី១៦ ខែមីនា ឆ្នាំ២០២០ ដល់ថ្ងៃទី១៥ ខែឧសភា ឆ្នាំ២០២០

តាក់តែងឡើងដោយ និស្សិតឈ្មោះ គង់ រក្សា សន សំខាន់ សាស្ត្រាចារ្យណែនាំ បណ្ឌិត លឹម សេងឌី

ឆ្នាំចូលសិក្សា ២០១៦ ឆ្នាំសរសេរសារណា ២០២០

ថ្នាក់បរិញ្ញាបត្រ	សេដ្ឋកិច្ចព័ត៌មានវិទ្យា
ជំនាន់ទី ១៥	

### សេចក្តីថ្លៃ១អំណរគុណ

យើងខ្ញុំឈ្មោះ **អខ់ អេតូ** និង **សន សំខាន់** ជានិស្សិតនៃមហាវិទ្យាល័យ សេដ្ឋកិច្ចព័ត៌មាន វិទ្យា ថ្នាក់បរិញ្ញាបត្រសេដ្ឋកិច្ចព័ត៌មានវិទ្យា ឆ្នាំទី៤ ជំនាន់ទី១៥ នៃសាកលវិទ្យាល័យភូមិន្ទនីតិ សាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច។

# សុមសម្ដែទទូទ**ភត្តញ្ញុតា**ឆទ៌ និទថ្លៃទងំណរគុណយ៉ាទទ្រាលទ្រៅ ទូនចំពោះ

លោកឪពុក អ្នកម្តាយ ដែលបានផ្តល់កំណើតចិញ្ចឹមបីបាច់ថៃរក្សា តាំងពីតូចរហូតមកដល់ ថ្ងៃនេះ អប់រំប្រៀនប្រដៅឲ្យស្គាល់ អ្វីខុស អ្វីត្រូវ ល្អ អាក្រក់ ស ឬខ្មៅ ជុំរុញលើកទឹកចិត្តក្នុងការ សិក្សា ហើយថែមទាំងជួយទំនុកបម្រុងសព្វគ្រប់បែបយ៉ាង ទាំងស្មារតី សម្ភារៈ និងថវិកា ដើម្បីផ្តល់ អោយយើងខ្ញុំមានលទ្ធភាពគ្រប់គ្រាន់ក្នុងការបន្តការសិក្សា ក្រេបយកចំណេះដឹង តាំងពីថ្នាក់មត្តេ យ្យសិក្សា រហូតដល់ឧត្តមសិក្សា។ លោកទាំងពីរបានខិតខំតស៊ូ នឿយហត់គ្រប់បែបយ៉ាងដើម្បីអោ យក្ខនៗមានចំណេះដឹងគ្រប់គ្រាន់ក្នុងការជួយទំនុកបម្រុងក្នុង គ្រូសារ និងសង្គមជាតិនៅពេលអ នាគត។

ឯកឧត្តម សាកលវិទ្យាធិកា សាកលវិទ្យាធិការង ព្រឹទ្ធបុរស ព្រឹទ្ធបុរសរង ប្រធាន ការិយាល័យស្រាវជ្រាវ សាស្ត្រាចារ្យ ព្រមទាំងបុគ្គលិកទាំងអស់ នៅក្នុងសាកលវិទ្យាល័យ ភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច ដែលបានចំណាយពេលវេលាដ៍មានតម្លៃដើម្បីខិតខំ

បង្ហាត់បង្រៀន ក៏ដូចជាណែនាំយើងខ្ញុំកន្លងមកយ៉ាងយកចិត្តទុកដាក់ និងអស់ពីកម្លាំងកាយចិត្ត។ លោកសាស្ត្រាចារ្យ **រើទ សេខឌី** ដែលជាសាស្ត្រាចារ្យណែនាំបានខិតខាំប្រឹងប្រែងអស់ពី កម្លាំងកាយចិត្ត ក្នុងការបង្ហាត់បង្រៀន ផ្តល់ជាចំណេះដឹង ឯកសារ គំនិត គន្លឹះល្អ ព្រមទាំងជួយកែ លម្អរាល់នូវកហុសឆ្គងទាំងឡាយរបស់យើងខ្ញុំ ដើម្បីចងក្រងជាសៀវភៅនេះឡើងតាំងពីដើមរហូត ដល់ចប់បានដោយជោគជ័យ។

មិត្តភក្តិទាំងអស់ ដែលបានសិក្សាជាមួយគ្នាកន្លងមក។ ពួកគេតែងតែផ្តល់ជាយោបល់ផ្សេង ក្នុងការសិក្សា និងជួយទុកធុរៈគ្នាទៅវិញទៅមកនៅពេលមានបញ្ហាផ្សេងៗ ហើយពួកគេក៏តែងតែ លើកទឹកចិត្តយើងខ្ញុំក្នុងការរៀបចំសៀវភៅនេះឡើងផងដែរ។

ជាចុងបញ្ចប់យើងខ្ញុំទាំងពីរ ស្ងមប្រសិទ្ធិពរជ័យជូនដល់ លោកអ្នកមានគុណទាំងពីរ ឯក ឧត្តម សាកលវិទ្យាធិកា សាកលវិទ្យាធិការង ព្រឹទ្ធបុរស ព្រឹទ្ធបុរសរង ប្រធានការិយាល័យស្រាវជ្រាវ សាស្ត្រាចារ្យ ព្រមទាំងបុគ្គលិកទាំងអស់នៅក្នុងសាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រ សេដ្ឋកិច្ច លោកសាស្ត្រាចារ្យ លឹម សេងឌី និងមិត្តភក្តិទាំងអស់ សូមអោយមានសុខភាពល្អ ទៅ ណាមកណាប្រកបដោយសុវត្ថិភាពគ្រប់ទីកន្លែង មានសុភមង្គលក្នុងក្រុមគ្រូសារ និងជួបប្រទះតែ ពុទ្ធពរទាំងបួនប្រការគឺ អាយុ វណ្ណៈ សុខៈ ពលៈ កុំបីឃ្លៀងឃ្លាតឡើយ។

#### សេរទ្ធភទា

ក្រោយពីបានបញ្ចាប់ការសិក្សាផ្នែកទ្រឹស្តីនៃជំនាញសេដ្ឋកិច្ចព័ត៌មានវិទ្យានៅសាកលវិទ្យា ល័យភូមិន្ទនីតិសាស្ត្រនិងវិទ្យាសាស្ត្រសេដ្ឋកិច្ចរយៈពេលជាងបីឆ្នាំកន្លងមកនេះយើងខ្ញុំបាន ចំណាយពេលវេលាក្នុងការសិក្សា ស្រាវជ្រាវនិងចងក្រងជាសៀវភៅនេះទ្បើងដែលជាការធ្វើការ ស្រាវជ្រាវលើប្រធានបទ៖ **ភារភារបារឆិតួន័យអូអច្រើប្រាស់អ្តុទម្រព័ន្ធលោអទីអ** ដើម្បី បញ្ជាក់ថាបានបញ្ចប់ថ្នាក់បរិញ្ញាបត្រផ្នែកសេដ្ឋកិច្ចព័ត៌មានវិទ្យានៅសាកលវិទ្យាល័យភូមិន្ទនីតិ សាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច។

ស្នាដៃនេះបានបង្កើតចេញពីការខិតខំប្រឹងប្រែងស្រាវជ្រាវរបស់យើងខ្ញុំទាំងពីររូប រូមសហ ការជាមួយសាស្ត្រាចារ្យណែនាំ ព្រមទាំងមិត្តភក្តិដែលជួយផ្តល់ជាមិតិផ្សេងៗ។ យើងខ្ញុំចងក្រង សៀវភៅនេះឡើង ដើម្បីជួយកាត់បន្ថយនូវហានិភ័យផ្សេងៗដែលមានការកើតឡើងនៅក្នុង បណ្តាញណែតវឹក និងព្រមទាំងការការពារទិន្នន័យរបស់អ្នកផងដែរ។ ហើយយើងទាំងពីរនាក់ក៏ មានបំណង លើកស្ទូយការធ្វើការស្រាវជ្រាវលើវិស័យព័ត៌មានវិទ្យាអោយកាន់តែច្រើនបន្តទៀតនៅ ក្នុងប្រទេសកម្ពុជា ដើម្បីទុកជាសមិតិផលដល់អ្នកស្រាវជ្រាវជំនាន់ក្រោយផងដែរ។

សៀវភោនេះក៏ជាគុណប្រយោជន៍របស់អ្នកស្រាវជ្រាវជំនាន់ក្រោយរបស់និស្សិត និងអ្នក ផ្សេងទៀត ដែលចង់សិក្សាស្វែងយល់ពីបច្ចេកវិទ្យាដែលមាននៅក្នុងផ្នែកព័ត៌មានវិទ្យា ហើយវាក៏ជា សមិតិផលដំបូងរបស់ព្លកខ្ញុំផងដែរ ទោះបីយើងខ្ញុំខិតខំធ្វើការសម្រិតសម្រាំង និងពិនិត្យម៉ត់ចត់ យ៉ាងណាក៏ដោយ ក៏យើងខ្ញុំនៅតែជឿជាក់ថាសៀវភៅមួយនេះនៅតែមានកំហុសឆ្គង ឬ ខ្វះចន្លោះ ដោយយថាហេតុ ឬដោយអចេតនាជាមិនខាន។

ជាទីបញ្ចប់ យើងខ្ញុំទាំងពីរនាក់ស្ងមប្រសិទ្ធិពរជ្ធនពរដល់អ្នកអានទាំងអស់ ទទូលបាននូវ ពុទ្ធពរទាំងប្ងូនប្រការនៅក្នុងជីវិតអ្នកទាំងអស់គ្នាតរៀងទៅ ទៅណាមកណាប្រកបដោយសុវត្ថិភាព និងមានសុភមង្គលនៅក្នុងគ្រូសារ។ ម្យ៉ាងវិញទៀតយើងខ្ញុំស្ងមទទួលការរិះគន់ និងកែលំអ ទាំងឡាយដោយក្តីសោមនស្ស ពីសំណាក់អ្នកអានទាំងអស់គ្នា។

# 

ຍາສື່ສາ

២. មូលដ្ឋាននៃការសិក្សាស្រាវជ្រាវ	. ១
៣. ការកំណត់បញ្ហានៃការស្រាវជ្រាវ	.២
វ.គោលបំណងនៃការស្រាវជ្រាវ	.២
វ. វិធីសាស្ត្រនៃការស្រាវជ្រាវ	.២
១. ដែនកំណត់នឹងវិសាលភាពនៃការសិក្សាស្រាវជ្រាវ	៣
៧. សារ:សំខាន់ក្នុងស្រាវជ្រាវ	៣
វ. រចនាសម្ពន្ធ័នៃការសិក្សាស្រាវជ្រាវ	៣

# ខំពូតនី១ តារសិត្សាន្រីស្តីមណ្តាញៈំណេតទ៉ឺត

9.9	មូលដ្ឋាននិងគោលការណ៍សន្តិសុខ (Security Concepts and Principles)៥
	១.១.១ ភាពសម្ងាត់ (Confidentiality)៥
	១.១.២ សុក្រឹតភាព (Integrity)៥
	១.១.៣ លទ្ធភាព (Availability)៥
	១.១.៤ មូលដ្ឋាននិងគោលការណ៍សន្តិសុខផ្សេងៗ (Others)៦
១.២	ម៉ូដែល OSI៦
ອ.	ឧបករណ៍បណ្តាញ (Network Devices) ៧
	១.៣.១ ឧបករណ៍ Hub ៧
	១.៣.២ ឧបករណ៍ Layer 2 Switchផ
	១.៣.៣ ឧបករណ៍ Bridge៩
	១.៣.៤. ឧបករណ៍ Router១០
	១.៣.៥ ច្រកបណ្តាញ (Gateway)១០

	១.៣.៦ ចំណុចអាក់សេស/អាក់សេសភ័ញ (Access Point/Wireless AP)	99
ອ.໔.	ការការពារបណ្តាញ (Network Defense)	99
	១.៤.១ ជញ្ញាំងភ្លើង (Firewall)ទ	១២
	១.៤.២ ប្រព័ន្ធអង្កេតល្មួច (Intrusion Detection System)១	១៣
	១.៤.៣ ប្រព័ន្ធបង្ការល្មួច (Intrusion Prevention System)ទ	១៤
	១.៤.៤ ប្រព័ន្ធត្រូតអាក់សេសបណ្តាញ (Network Access Control System/NAC) ទ	១៥
	១.៤.៥ ចម្រោះវេប (Web Filter)ទ	១៦
	១.៤.៦ សេវូបករណ៍ Proxy (Proxy Server)ទ	១៦
	១.៤.៧ អង់ទីម៉ាល់វែរ (Anti-malware)ទ	១៦
១.៥	ប្រភេទអង្គត់បណ្តាញ (Network Segment Types)ទ	១៧
	១.៥.១ បណ្តាញសាធារណ: (Public Network)	១៧
	១.៥.២ បណ្តាញឯកជន (Private Network)ទ	១៧
	១.៥.៣ បណ្តាញកូនកាត់ (semi-public Network)	១៨
	១.៥.៤. បណ្តាញតំបន់ស (Demilitarized Zone-DMZ)	១៨

# ෫෯෪ඁ෭෨ඁ

# នៃឧភាអេនុទត្តនំគម្រោទ

២.១ បរិយាយទូទៅនៃគម្រោង	១៩
២.២ ផែនការកាលវិភាគនិងភារកិច្ច	១៩
២.៣ លក្ខខណ្ឌនិងតម្រវការសម្ភារ: (Security Testing)	២០
២-៤. លទ្ធផលរំពឹងទុក	ህ០

# ຮໍດູສສັດ

# **ໍ**ຂໍເສງິອ**ຂີອ**ຮອໍ່ສະອື່ສອຍໝາញ

២១	សន្តិសុខបណ្តាញ (Network Security)	៣.១
២១	៣.១.១ របៀបនៃការដំណើរជញ្ជាំងភ្លើង (Firewall)	
r)២៧	៣.១.២ របៀបនៃការដំឡើង វេប វៀលធើ (Web Filter	

៣.២	សន្តិសុខអាក់សេសភ័ញ (Access Point Security)	៣២
៣.៣	សន្តិសុខរីនដ្ធ (Endpoint Windows Security)ព	ណ ផ
	៣.៣.១ អេក្រង់ឆ្លាតរបស់ Windows Defender (Smart Screen)	ភា ៥
	៣.៣.២ កម្មវិធីឆ្នាំរបស់ Windows Defenderព	៣៧
	៣.៣.៣ លក្ខណះ User Account Control	៤០
	៣.៣.៤ ឆ្នាំឧបករណ៍របស់ Windows Defender	៤១
	៣.៣.៥ ឆ្នាំ Exploit វបស់ Windows Defender	៤៥
	៣.៣.៦ Microsoft Bitlocker	៥ ០
	៣.៣.៧ ឆ្នាំ Credential របស់ Windows Defender	៥ ២
៣.៤	តេស្តសន្តិសុខ (Security Testing)	៥៦
	៣.៤.១ Nmap	៥៦
	៣.៤.២. Nessus	៥៨

# សេចភ្លីសត្ថិដ្ឋាន និច ភាវផ្តល់អនុសាសន៍

9. I	សេចក្តីសន្និដ្ឋាន	៦៥
២. i	ការផ្តល់អនុសាសន៍	៦៥

#### ຉຆຎຎຎຎ

# ទញ្ជ័រូមនាព

រូបភាពទី១៖ បង្ហាញពីស្រទាប់ OSI Model	៧
រូបភាពទី២៖ បង្ហាញពីឧបករណ៍ Hub	៨
រូបភាពទី៣៖ បង្ហាញពីឧបករណ៍ Switch	3
រូបភាពទី៤៖ បង្ហាញពីឧបករណ៍ Bridge	3
រូបភាពទី៥៖ បង្ហាញពីឧបករណ៍ Routers	90
រូបភាពទី៦៖ បង្ហាញពីឧបករណ៍ Gateway	99
រូបភាពទី៧៖ បង្ហាញពីឧបករណ៍ Wireless Access Point	99
រូបភាពទី៨៖ រូបភាពទី៨៖ បង្ហាញពីជញ្ជាំងភ្លើងឬ Firewall	១២
រូបភាពទី៩៖ បង្ហាញពីការតប្រព័ន្ធបណ្តាញទ	១៣
រូបភាពទី១០៖ បង្ហាញពីការរៀបចំប្រព័ន្ធដើម្បើអង្កេតពីការជ្រៀតចូលនៃ Viruses	១៤
រូបភាពទី១១៖ បង្ហាញពីការរៀបចំប្រព័ន្ធដើម្បើបង្ការពីការជ្រៀតចូលនៃ Viruses	១៥
រូបភាពទី១២៖ បង្ហាញពីប្រព័ន្ធ Network Access Control System	១៦
រូបភាពទី១៣៖ បង្ហាញពី Network Segment Typesទ	១៧
រូបភាពទី១៤៖ បង្ហាញពីដ្យាក្រាមនៃបណ្តាញសន្តិសុខ Network	២១
រូបភាពទី១៥៖បង្ហាញពីការបើក Firewall នៅលើ Router	២២
រូបភាពទី១៦៖ បង្ហាញពីការការកំណត់ទៅលើ Local Managementលើ Firewall	២២
រូបភាពទី១៧៖ បង្ហាញពីការបើកដំណើការលើ Access Control២	ៗ៣
រូបភាពទី១៨៖ បង្ហាញពីការ Add New Host នៅលើ Access Control២	ៗ៣
រូបភាពទី១៩៖ បង្ហាញពី Mac Address នៅលើ Access Control	២៤
រូបភាពទី២០៖ បង្ហាញពីការកំពត់ទៅលើ Target នៅលើ Access Control	២៤
រូបភាពទី២១៖ បង្ហាញពីការកំណត់ Scheduleនៅលើ Access Control	ሮ
រូបភាពទី២២៖ បង្ហាញពីការកំណត់ Rule នៅលើ Access Control	ሮ
រូបភាពទី២៣៖ បង្ហាញពីការ Add New Rule នៅលើ Access Control	២៦
រូបភាពទី២៤៖ បង្ហាញពីដំណាក់កាលចុងក្រោយពេលដំឡើងរូច	២៦
រូបភាពទី២៥៖ បង្ហាញពីបង្ហាញអំពីការចូលក្នុងរោតទ័រតាម Web Browser l	ៗ៧
រូបភាពទី២៦៖ បង្ហាញអំពីការវាយឈ្មោះអ្នកប្រើប្រាស់នឹងលេខសម្ងាត់	ៗ៧

រូបភាពទី២៧៖ បង្ហាញអំពីការជ្រើសរើសនូវច្បាប់ Website Filter	.២៧
រូបភាពទី២៨៖ បង្ហាញអំពីការជ្រើសរើសនូវ Access Control	២៨
រូបភាពទី២៩៖ បង្ហាញអំពីការចុចពាក្យ Next នៅលើ Add New Policy	២៨
រូបភាពទី៣០៖ បង្ហាញអំពីការវាយពាក្យ Website Filter ក្នុង Policy Name	២៩
រូបភាពទី៣១៖បង្ហាញអំពីការវាយពាក្យ Always នឹង ជ្រើសរើស Always	២៩
រូបភាពទី៣២៖ បង្ហាញអំពីការវាយ Address Type នឹង IP Address	.៣០
រូបភាពទី៣៣៖ បង្ហាញអំពីការជ្រើសរើសយក Apply Web Filter	.៣០
រូបភាពទី៣៤៖ បង្ហាញអំពីការជ្រើសរើសយក Disable ឬ Enable	. ៣១
រូបភាពទី៣៥៖ បង្ហាញអំពីការរក្សាទុកនៃ Website Filter	. ៣១
រូបភាពទី៣៦៖ បង្ហាញអំពីការបើកដំណើរការ Access Point Security	.៣២
រូបភាពទី៣៧៖ បង្ហាញអំពីការប្តូរ និងConfigureនៅលើAccess Point Security	.៣៣
រូបភាពទី៣៨៖ បង្ហាញអំពីការ Configureនៅក្នុង WEP នៅលើAccess Point Security	. ៣៤
រូបភាពទី៣៩៖ ៖ បង្ហាញអំពីដំណាក់កាលក្រោយConfigure នៅលើAccess Point Security	. ៣៤
រូបភាពទី៤០៖ បង្ហាញពីផ្ទាំង Search Engine	. ៣៦
រូបភាពទី៤១៖ បង្ហាញពីផ្ទាំង Setting	. ៣៦
រូបភាពទី៤២៖ បង្ហាញផ្ទាំងនៃ Window Security	.៣៧
រូបភាពទី៤៣៖ បង្ហាញការបើដំណើរការនៃ SmartScreen	.៣៧
រូបភាពទី៤៤៖ បង្ហាញអំពីផ្ទាំង Search Engine	. ៣៨
រូបភាពទី៤៥៖ បង្ហាញអំពីផ្ទាំង Security at a glance	. ៣៩
រូបភាពទី៤៦៖ បង្ហាញអំពីផ្ទាំង Virus & Threat Protection	. ៣៩
រូបភាពទី៤៧៖ បង្ហាញអំពីការបើកដំណើរការ Window Defender	d O
រូបភាពទី៤៨៖ បង្ហាញពីការស្វែងរកនៃ UAC	๔ ១
រូបភាពទី៤៩៖ បង្ហាញពីការជ្រើសរើសនៃការប្រើប្រាស់ UAC	๔ ១
រូបភាពទី៥០៖ បង្ហាញពី Edit Group Policy	៤២
រូបភាពទី៥១៖ បង្ហាញពី Local Group Policy Editor	.៤៣
រូបភាពទី៥២៖ បង្ហាញពី Administrative ក្នុង Local Group Policy Editor	.៤៣
រូបភាពទី៥៣៖ បង្ហាញពី Window Components	៤ ៤

រូបភាពទី៥៤៖ បង្ហាញពីផ្ទាំង Window Defender Application Guard	d d
រូបភាពទី៥៥៖ បង្ហាញពីផ្ទាំងពីការបើកនៃ Window Application Guard	៤ ៥
រូបភាពទី៥៦៖ បង្ហាញពីផ្ទាំងពីការបើកនៃ Window Application Guard	៤ ៥
រូបភាពទី៥៧៖ បង្ហាញពី Edit Group Policy	៤៦
រូបភាពទី៥៨៖ បង្ហាញពី Local Group Policy Editor	๔๗
រូបភាពទី៥៩៖ បង្ហាញពី Administrative ក្នុង Local Group Policy Editor	๔๗
រូបភាពទី៦០៖ បង្ហាញពី Window Components	៤៨
រូបភាពទី៦១៖ បង្ហាញពី Window Defender Exploit Guard	៤៨
រូបភាពទី៦២៖ បង្ហាញពី Exploit	៤ ៩
រូបភាពទី៦៣៖ បង្ហាញពី Use a common set of exploit protection	໔ ៩
រូបភាពទី៦៤៖ បង្ហាញពី Enable Window Defender Exploit Guard	៥ O
រូបភាពទី៦៥៖ បង្ហាញពី Manage BitLocker	៥១
រូបភាពទី៦៦៖ បង្ហាញពី Turn On BitLocker	៥១
រូបភាពទី៦៧៖ បង្ហាញពី Edit Group Policy	ሬ ሀ
រូបភាពទី៦៨៖ បង្ហាញពី Local Group Policy Editor	៥៣
រូបភាពទី៦៩៖ បង្ហាញពី Administrative ក្នុង Local Group Policy Editor	៥៣
រូបភាពទី៧០៖ បង្ហាញពី System នៅក្នុង Local	៥៤
រូបភាពទី៧១៖ បង្ហាញពី Device Guard នៅក្នុង Local Group Policy	៥៤
រូបភាពទី៧២៖ បង្ហាញពី Turn on Virtualization Based Security	ሮ ሮ
រូបភាពទី៧៣៖ បង្ហាញពី Enable Window Defender Credential Guard	៥ ៥
រូបភាពទី៧៤៖ បង្ហាញពីការ Install nmap នៅលើ Window	៥៦
រូបភាពទី៧៥៖ បង្ហាញពីការ Install nmap នៅលើ Window	៥៦
រូបភាពទី៧៦៖បង្ហាញពីការ Install nmap នៅលើ Window	៥៧
រូបភាពទី៧៧៖ បង្ហាញពីការ Install nmap នៅលើ Window	៥៧
រូបភាពទី៧៨៖បង្ហាញពីការ Install nmap នៅលើ Window	៥៨
រូបភាពទី៧៩៖ បង្ហាញពីការ Install nmap នៅលើ Window	៥៨
រូបភាពទី៨០៖ បង្ហាញអំពីការដោតឡូត ស្ងហ្វ៊ែ Nessus	៥៨

រូបភាពទី៨១៖ បង្ហាញអំពី File Of Nessus	. ៥៩
រូបភាពទី៨២៖ បង្ហាញអំពីការដោតឡូត សូហ៊្វែ Nessus	. ៥៩
រូបភាពទី៨៣៖ បង្ហាញអំពីការព្រមនៃការដោតទ្បូត ស្ងហ្វ៊ៃ Nessus	. ៥៩
រូបភាពទី៨៤៖ បង្ហាញអំពីការព្រមនៃការដោតឡូត ស្ងហ្វ៊ែ Nessus	.៦០
រូបភាពទី៨៥៖ បង្ហាញអំពីការព្រមនៃការដោតឡ្យ៉ូត ស្ងហ្វ៉ែ Nessus	.៦០
រូបភាពទី៨៦៖ បង្ហាញអំពីការព្រមនៃការដោតឡ្យ៉ូត ស្ងហ្វ៉ែ Nessus	.៦១
រូបភាពទី៨៧៖ បង្ហាញអំពីផ្ទាំង ស្ងហ្វ៊ែ Nessus នៅក្នុង Web Browser	.៦១
រូបភាពទី៨៨៖ បង្ហាញអំពីផ្ទាំង Processed to LocalHost	.៦២
រូបភាពទី៨៩៖ បង្ហាញអំពីការជ្រើសរើស Nessus Essential	.៦២
រូបភាពទី៩០៖ បង្ហាញអំពីការវាយ Register Nessus	៦៣
រូបភាពទី៩១៖ បង្ហាញអំពីការវាយ Username & Password	៦៣
រូបភាពទី៩២៖ បង្ហាញអំពីផ្ទាំងនៃការស្វែងរក Nessus Scan	. ៦៤

# សេខភ្គីឆ្អើន

# 

នាពេលបច្ចុប្បន្ននេះ យើងដឹងហើយថាពិភពលោកមានការអភិវឌ្ឈន៍យ៉ាង ឆាប់រហ័សនៅ គ្រប់វិស័យជាពិសេសដូចជាវិស័យបច្ចេកវិទ្យាព័ត៌មានវិទ្យា ដែលបានដើរតូនាទីយ៉ាងសំខាន់មួយ ក្នុងការធ្វើឲ្យមានទំនាក់ទំនងរវាងគ្នានឹងគ្នា។ តាមរយៈការរីកចម្រើននេះធ្វើឲ្យ វាមានភាពកាន់តែ ងាយស្រូលក្នុងការទំនាក់ទំនងយ៉ាងរហ័សមួយផងដែរ។ ដោយសារតែការប្រើប្រាស់បច្ចេកវិទ្យា ព័ត៌មានវិទ្យា មានភាពទំលំទូលាយ បែបនេះហើយ ទើបមានការប្រើប្រាស់ មុខងារ ជាច្រើន តាមរយៈការប្រើប្រាស់បញ្ហាណណែតវ៉ឹក សម្រាប់ការដែលមានប្រយោជន៍សម្រាប់ស្តាបន័ជា ច្រើន ។ តាមការប្រើប្រាស់ ប្រព្ធន័បណ្តាញណែតវ៉ឹកដែលមានលក្ខណៈដូចជា បណ្តាញណែតវ៉ឺ ក លក្ខណតូច បណ្តាញណែតវ៉ឹកលក្ខណៈមធ្យម នឹង បណ្តាញណែតវ៉ឹកលក្ខណៈទំលំទូលាយ ។ ការប្រើប្រាស់បណ្តាញណែតវ៉ឺក វាមានភាពប្រហាក់ប្រហែលគ្នាច្រើន ដូចជាអាចគ្រប់គ្រង់ ទិន្នន័យពីការវាយប្រហារពីជនខិលខ្ទចខាងក្រៅ ងាយស្រួលក្នុងការផ្ទេរទិន្នន័យច្រើននឹងការងារ ដែលមានប្រយោជន៍ជាច្រើនទៀត។ ដោយសារកត្តាទាំងនេះដែលអាចធ្វើឲ្យស្ថាបន័រដ្ឋ នឹងឯក ជនជាច្រើន ប្រើប្រាស់ប្រព្ធន័មួយនេះស្ទើរតែគ្រប់ផ្នែកទាំងអស់ក្នុងស្តាបន័របស់ព្លកគេ ។ ហេតុ ដូចនេះហើយ ទើបធ្វើឲ្យក្រុមរបស់ខ្ញុំមានគំនិត ក្នុងការសិក្សាស្រាវជ្រាវអំពីប្រព្វន័ណែតរ៉ឹក ដែល ជាបច្ចេកវិទ្យាមួយដែល មានភាពងាយស្រុសក្នុងការធ្វើឲ្យមានទំនាក់ទំនង នឹងសិក្សាស្រាវជ្រាវ អំពីសុវត្ថិភាពក្នុងការដឹងពីប្រើប្រាស់ប្រព្ធន័ណែតវ៉ឹកមួយនេះ ឲ្យប្រសិទ្ធភាព តាមរយៈវិធានបទ ៉ ការការពារប្រព្ធន័សុវិត្តភាពណែតវ៉ឹក ″ ដែលជំរុញឲ្យមានការការពារទុកជាមុនក្នុងការប្រើប្រាស់ ណែតវ៉ឺកឲ្យមានសុវត្ថិភាព នឹងប្រសិទ្ធភាពមួយ។

## ២. ຮູ໙ຊຼາຂໄຂສາເຜີສຸດເພຍອງອາຮ

តាមរយៈការប្រើប្រាស់បណ្តាញណែតវ៉ឹក តែងតែមានការរំខានពីជនខិលខ្ទួចដែលព្យាយាម លួចយកឯកសាររបស់យើង ដូចនេះការការពារប្រព្ធន័សុវត្ថិភាពណែកវ៉ឹក គឺជាកត្តាមួយដែលអាច ធានាបាននូវសុវត្ថិភាពទិន្នន័យរបស់អ្នកកំឡុងពេលដែលអ្នកប្រើប្រាស់បណ្តាញណែតវ៉ឹកឲ្យមាន ភាពល្អប្រសើរ។ លើសពីនេះទៅទៀតអ្នកគ្រប់គ្រង់លើប្រព្ធន័នេះអាចប្រើប្រាស់ប្រព្ធន័បណ្តាញ ណែតវ៉ឹកនេះសម្រាប់ការគ្រប់គ្រង់ ឬអាចបញ្ហូ ព្រមទាំងអាចអនុញ្ញាតឲ្យត្រឹមតែអ្នកប្រើប្រាស់បាន ប្រើប្រាស់នូវទំហំការងាររបស់ពួកគេតែប៉ុណ្ណោះ ដោយមិនអនុញ្ញាតឲ្យអ្នកប្រើប្រាស់អាចធ្វើអ្វី ដែលមានផលប៉ះពាល់ដល់ប្រព្វន័ណែតរ៉ឹកនោះឡើយ។

# ๓. ສາເສໍ້ໝສ່ຍຫຼາໂຂສາເໜອງອາອ

ផ្អែកទៅការសិក្សាស្រាវជ្រាវលើការប្រើប្រាស់បណ្ដាញណែតវ៉ឹក វាតែងតែកើតឡើងនូវបញ្ហា មួយចំនួនដែលភាគច្រើនបង្ករឡើងដោយពួក HACKER ដែលតែងតែរំខាន វាយប្រហារ នឹងល្ងច ទិន្នន័យនៅតាមបណ្ដាញណែតវ៉ឹកដែលបានប្រើប្រាស់។ ជនទាំងនេះតែងតែប្រើប្រាស់នូវកម្មវិធី ដែលមានផ្ទុកមេរោគ ដើម្បីផ្សាយមេរោគទាំងអស់នេះក្នុងកុំព្យូទ័រ រួចក៍គ្រប់គ្រង់រាល់សកម្មភាព ដែលយើងបានប្រតិបត្តិ។ ហើយមេរោគទាំងនេះវាអាចជ្រៀតចូលបាននៅពេលដែលយើងមិន មានការប្រុងប្រយ្នត័នៅពេលដែលយើងបានប្រើប្រាស់ អ៊ិនធឺណែត ឬមានការធ្វេសប្រហេសក្នុង ប្រការណាមួយ ដូចជាការ ទាញកម្មវិធី ដែលមានមេរោគពីប្រព្វន័អ៊ិនធឺណែត។ ព្រមទាំង ការប្រើប្រាស់ប្រព្វន័ អ៊ិនធឺណែតដោយគ្មានឧបករណ៍ ទប់ស្កាត់ពីការវាយប្រហាររបស់ ATTACKER ដូចជាឧបករណ៍ការពារ CISCO FIREWALL ជាដើម។

# ເສານອໍາເນອງເຮົາສາງຄາອງຊາອ

តាមរយៈនៃការស្រាវជ្រាវលើផ្អែកណែតរ៉ឺក ក្រុមយើងខ្ញុំមើលឃើញនូវការប្រើប្រាស់នូវ Tools មួយចំនួនសម្រាប់តំឡើង ដើម្បីការពារនូវសុវត្ថិភាពទិន្នន័យ ក៍ដូចជាកាត់បន្ថយនូវការវាយ ប្រហារនានាពី ATTACKER ព្រមទាំងអាចគ្រប់គ្រង់នូវអ្នកប្រើប្រាស់មានស្វិទ្ធត្រឹមតែអាចធ្វើកិច្ច ការរបស់ពួកគេតែប៉ុណ្ណោះ។ ខាងក្រោមនេះជាចំណុចសំខាន់ៗដែលយើងបានសិក្សាស្រាវជ្រាវ៖

- គ្រប់គ្រង់ទៅលើគណនីអ្នកប្រើប្រាស់ និង កំណត់សិទ្ធិប្រើប្រាស់
- > ការពារលើ បណ្តាញណែតវ៉ឹកធុរកិច្ចតូចៗ
- >ការការពារទៅលើទិន្នន័យរបស់អ្នកប្រើប្រាស់
- ធ្វើការតំឡើង បណ្តាញណែតវ៉ឹកនៅក្នុងផ្ទះ

# ៥. ទិធីសាស្ត្រនៃការស្រាទខ្រាទ

ក្រោយពីការវិភាគ ក៍ដូចជាការសិក្សាស្រាវជ្រាវទៅលើប្រធានបទខាងលើនេះ យើងមានវិធី សាស្ត្រដែល គ្រាំទ្រលើ ការសិក្សា បែប រុករកឯកសារ ដែលមានក្នុង បណ្ណាល័យ ក្នុងបណ្តា ញរអ៊ីនធើណែត ក៍ដូចជាឯកសារដែលបានសិក្សាម្តងរូចមកហើយ ដែលជាប្រភពសំខាន់ក្នុងការ គ្រាំទ្រលើប្រធានបទរបស់យើងខាងលើនេះ។យើងបានចែកជាដំណាក់កាលក្នុងការធ្វើវិធីសាស្ត្រ ក្នុងការស្រាវជ្រាវដែលអាចនាំឲ្យយើងមានភាពងាយស្រ<sub>្</sub>លសម្រាប់ប្រធានបទរបស់យើង។ ដំណាក់កាលទាំងនោះរូមមាន៖

- ស្វែងយល់ពីចំណុចខ្សោយនៃណែតរ៉ឺក ដែលយើងត្រូវការពារ
- រៀបរៀងរាល់សំណូរដែលពាក់ព្ធន័លើការការពារប្រព្ធន័ណែតរ៉ឺក
- ការស្វែងរកឯកសារដែលមានក្នុងបណ្ណាល័យ នឹង ប្រព្ធន័ណែតវ៉ឺក
- ការអនុវត្តលើការវាយប្រហារ នឹងការការពារលើកម្មវិធីផ្សេងៗ

# ៦. ເຂລສໍฌສຂຶອອີຄາແສາຕໄຂສາເພື່ສຸງເທາອາຍາອ

ផ្នែកទៅតាមពេលវេលានៃការសិក្សាស្រាវជ្រាវលើប្រធានបទខាងលើ ដែនកំណត់នៃការ យល់ដឹងនៃការការពារប្រព្ធន័ណែតវ៉ឹកយើងអាចត្រឹមតែបាននូវចំណុចស្នូលខ្លះៗ នៃប្រធានបទ ខាងលើនេះផងដែល ដូចជា ការការពារលើប្រព្ធន័កុំព្យូទ័រ ការដាក់ប្រព្ធន័លេខសម្ងាត់ដែលខ្លាំង ការបើកដំណើរការនៃ FIREWALL នឹង WINDOW DEFENDER ជាដើម ។ ការសិក្សាលើការដាក់ COMMAND នៅលើឧបករណ៍ដែលបានប្រើប្រាស់ក្នុងប្រព្ធន័ណែតវ៉ឹក។ ចំពោះវិសាលភាពនៃការ សិក្សាស្រាវជ្រាវរបស់ក្រុមយើងខ្ញុំ គ្រាន់តែផ្តោតសំខាន់លើ ហាងកាហ្វេតូចតាច នឹង លើក្រុម ហ៊ិនកំរិតតូចតែប៉ុណ្ណោះ ។

# ဂ). ရား:မံခာင်ခုံချွေရာချောခ

ផ្អែកលើការសិក្សាស្រាវជ្រាវលើប្រធានបទខាងលើយើងបានរួមនូវសារៈសំខាន់មួយចំនួន ដែលល្អក្នុងការការពារ ប្រព្ធន័សុវត្ថិភាពណែតវ៉ឹកដូចជា៖

- ការពាររាល់ទិន្នន័យដែលបានផ្ញើរតាមរយៈអ៊ីនធើណែត កុំឲ្យមានការបាត់បង់
- ការពារផ្ទាល់ទិន្នន័យក្នុងកុំព្យូទ័រ
- បង្កើននូវការប្រុងប្រយ្នត់ក្នុងការប្រើប្រាស់ប្រព្ធន៍ណែតរ៉ឹក

# ៤ ខេនាសម្ពន្ល៍នៃការសិក្សាស្រាទខ្រាទ

ដើម្បីសិក្សាពីប្រធានបទខាងលើនេះ យើងរៀបរចនាសម្ពន្ធ័ជាចំណុចធំៗបី គឺ ការសិក្សាលើ សេចក្តីផ្តើមការសិក្សាលើទ្រឹស្តីនៃណែតវ៉ឹក ការសិក្សាពីការការពារលើប្រព្វន័ណែតវ៉ឹក ។

> ការសិក្សាលើសេចក្តីផ្តើម

- កំណត់បញ្ហានៃប្រព្ធន័ណែតវ៉ឹក
- ស្វែងរកគោលបំណងនៃការការពារ
- ដឹងពីសារ:ប្រយោជន៍នៃការការពារណែតវ៉ឺក
- > ការសិក្សាលើទ្រឹស្តីនៃណែតវ៉ឹក
  - ស្គាល់ពីប្រភេទនៃណែតវ៉ឺក
  - ស្គាល់ពីប្រភេទឧបករណ៍នៃការប្រើ
- >ការសិក្សាលើការពារលើប្រព្វន័ណែតវ៉ឹក
  - ការពារកុំព្យូពីជ្រៀតចូលនៃប្រភេទនៃមេរោគ
  - ការពារទិន្នន័យរបស់កុំព្យូទ័រលើអ៊ីនធើណែត

# ខំពុភនី១ ភារសិភ្សាឆ្រីស្តីបណ្តាញលោតទុំភ

### **១.១ ទូលខ្ជានតិចឝោលអារេភ៍សត្តិសុខ** (Security Concepts and Principles)

គោលបំណងនិងវត្ថុបំណងសំខាន់នៃ សន្តិសុខប្រព័ន្ធព័ត៌មាន គឺស្ថិតនៅលើគោលការណ៍ សន្តិសុខបីគឺ ភាពសម្ងាត់ សុក្រឹតភាព និង លទ្ធភាព (CIA Triad)។

#### 9.9.9 ສາຕະອາສິ (Confidentiality)

គោលការណ៍សំខាន់ទី១នៃគោលការណ៍សន្តិសុខប្រព័ន្ធព័ត៌មានគឺភាពសង្ងាត់។ ភាពសម្តាត់ គឺជាការថៃរក្សាការសម្ងាត់ឬឯកជនភាពរបស់បុគ្គលឬស្ថាប័ន ដើម្បីធានាថាព័ត៌មានសំខាន់ៗអាច អាក់សេសបាន លុះត្រាតែមានសិទ្ធិ។ វាជាគំនិតមួយនៃវិធានការណ៍សន្តិសុខដែលត្រូវបានប្រើ ដើម្បីធានាការការពារការសម្ងាត់ទិន្នន័យ វត្ថុ ឬ ធនធាននៅលបណ្តាញកុំព្យូទ័រឬប្រព័ន្ធ។ គោល ដៅនៃការ ការពារភាព សម្ងាត់គឺ ដើម្បី ការពារឬកាត់បន្ថយ អាក់សេស ទិន្នន័យដោយ គ្មានការ អនុញ្ញាត។

### **១.១.២ សុទ្រីឥតរាព** (Integrity)

គោលការណ៍សំខាន់ទី២នៃគោលការណ៍សន្តិសុខប្រព័ន្ធព័ត៌មានគឺសុក្រឹតភាព។ វាជាភាព ត្រឹមត្រូវនៃព័ត៌មានដែលទទួលបានធៀបនឹងព័ត៌មានដើមដែលផ្ទុកក្នុងកុំព្យូទ័រ ជាពិសេស ពេល ធ្វើចរាចរណ៍លើបណ្តាញកុំព្យូទ័រ។ សុក្រឹតភាពគឺជាគំនិតនៃការការពារភាពជឿជាក់និងភាពត្រឹម ត្រូវនៃទិន្នន័យ។ ការការពារសុក្រឹតភាព រារាំងការផ្លាស់ប្តូរទិន្នន័យដែលគ្មានការអនុញ្ញាត។ វា ធានាថាទិន្នន័យនៅតែត្រឹមត្រូវ មិនផ្លាស់ប្តូរ និង រក្សាទុក។

អនុវត្តន៍ការការពារសុក្រឹតភាពបានត្រឹមត្រូវ ផ្តល់នូវមធ្យោបាយប្រឆាំងនឹងសកម្មភាពដែល គ្មានការអនុញ្ញាតនិងព្យាបាទ ក៏ដូចជាអ្នកប្រើប្រាស់ដែលមានការអនុញ្ញាត។

### **១.១.៣ សន្លនាព** (Availability)

គោលការណ៍សំខាន់ទី៣នៃគោលការណ៍សន្តិសុខប្រព័ន្ធព័ត៌មានគឺលទ្ធភាព។ លទ្ធភាពគឺជា ភាពមានសេវា ឬ ភាពដែលអាចប្រើប្រាស់បាន។ លទ្ធភាពមានន័យថា ប្រភព (source) ដែល មានការអនុញ្ញាត អាចធ្វើការអាក់សេសធនធាគ្រប់ពេលវេលានិងមិនមានការរំខាន។ ប្រសិនបើ យន្តការសន្តិសុខផ្តល់នូវ «លទ្ធភាព» វាធានាថា ទិន្នន័យ វត្ថុ និងធនធានអាចធ្វើការអាក់សេស បានចំពោះអ្នកដែលមានការអនុញ្ញាត។

#### 9.9.໔ ෂූහසුබබබිවເຮັດເຮັດເຮັດເຮັດເຮັດເຊິ່ງຍາງ (Others)

ក្រៅពីមូលដ្ឋានិងគោលការណ៍ទាំងបីនៃសន្តិសុខប្រព័ន្ធព័ត៌មានខាងលើ នៅមានមូលដ្ឋាន និងគោលការណ៍សន្តិសុខដទៃទៀតដូចជា ឯកជនភាព(Privacy) អត្តសញ្ញាណកម្ម (Identification) យឋាភូតកម្ម(Authentication) អនុញ្ញាត(Authorization) សវនាការ(Auditing) គណនេយ្យភាព(Accountability) និង non-repudiation ា

#### **១.២ ឌ៉ូខែល** OSI

គមនាគមន៍រវាងកុំព្យូទ័រលើបណ្តាញអាចធ្វើទៅបានដោយសារវិធីការ (Protocol)។ វិធីការគឺ ជាសំណុំក្បួនច្បាប់និងការរឹតត្បិតដែលកំណត់ពីរបៀបដែលទិន្នន័យត្រូវបានបញ្ហូនតាមមេឌាប ណ្តាញ (Network Medium)។ នៅដំណាក់កាលដំបូងនៃការអភិវឌ្ឍន៍បណ្តាញ ក្រុមហ៊ុនជាច្រើន មានវិធីការរៀងៗខ្លួន ដែលមានន័យថា អន្តរកម្មរវាងកុំព្យូទ័ររបស់ក្រុមហ៊ុនផ្សេងៗគ្នាច្រើនតែមិន អាចទាក់ទងជាមួយគ្នាបាន។ ដើម្បីលុបបំបាត់បញ្ហានេះ អង្គការស្តង់ដាអន្តរជាតិ (ISO) បាន បង្កើតម៉ូដែល OSI សម្រាប់វិធីការនានាឆ្នាំ១៩៨០ ។ ជាពិសេសOSI-៧៤៩៨ ត្រូវបានកំណត់ថា ជាម៉ូដែល OSI។

ម៉ូដែល OSI បែងចែកភារកិច្ចបណ្តាញជាប្រាំពីរស្រទាប់ផ្សេងគ្នា។ ស្រទាប់នីមួយៗទទួល ខុសត្រូវសម្រាប់អនុវត្តការងារជាក់លាក់ឬប្រតិបត្តិការសម្រាប់គមនាគមន៍រវាងកុំព្យូទ័រពីរ។ ស្រទាប់ទាំងនេះតែងតែរាប់ចាប់ពីក្រោមទៅលើ (ស្ងមមើលរូបភាព ១១.១)។ ឧទាហរណ៍ ស្រទាប់ទី៣ ត្រូវបានគេស្គាល់ថាជាស្រទាប់បណ្តាញ។ ស្រទាប់នីមួយៗទាក់ទងដោយផ្ទាល់ ជាមួយស្រទាប់ខាងលើឬស្រទាប់ខាងក្រោមវា បូករូមនឹងស្រទាប់នៅលើប្រព័ន្ធដៃគូទំនាក់ទំនង របស់វា។

5



#### រូបភាពទី១៖ បង្ហាញពីស្រទាប់ OSI Model

#### ១.៣ ឧទទារស៍មណ្តាញ (Network Devices)

ដើម្បីបង្កើតបណ្តាញកុំព្យូទ័រមួយ យើងត្រូវការឧបករណ៍ជាច្រើន ដូចជាកុំព្យូទ័រ ទូរស័ព្ទឆ្លាត ផ្នោះពុម្ព។ ឧបករណ៍ដែលសំខាន់និងចាំបាច់សម្រាប់ភ្ជាប់ឧបករណ៍ដូចជា កុំព្យូទ័រ ទូរស័ព្ទឆ្លាត ផ្នោះពុម្ព ស្ពែនន័យ ជាដើម ចូលគ្នាហៅថាឧបករណ៍បណ្តាញ។

#### **9.ຓ.9 ຂອສເຄລົ່** Hub

Hub ជាចំណុចតំណរូមមួយសម្រាប់ភ្ជាប់គ្រប់ឧបករណ៍ក្នុងបណ្តាញ។ Hub ភ្ជាប់អង្កត់លែន (LAN Segment) ចូលគ្នា មានច្រើនច្រក (Ports) និង ធ្វើការនៅស្រទាប់ទី១នៃម៉ូដែល OSI។ ពេលដុំទិន្នន័យមួយមកដល់ច្រកមួយ វាចម្លងទៅគ្រប់ច្រកទាំងអស់ ដើម្បីឱ្យអង្កត់នៃលែនទាំង អស់អាចមើលឃើញដុំទិន្នន័យនោះ។ វាបញ្ជូនដុំនោះទៅគ្រប់ច្រកទាំងអស់ ដោយពឹងផ្អែកលើ ព័ត៌មាននៅស្រទាប់ទី១ (ប៊ីតឬសញ្ញា) ។ ការបញ្ជូននេះបណ្តាលឱ្យមានដែនប៉ះទង្គិចធំ (Collision Domain) និង ដែនផ្សព្វផ្សាយធំ (Broadcast domain) ក្នុងបណ្តាញ។ ច្រកនីមួយៗនៃ Hub មាន ល្បឿនកំណត់មួយដែលអាស្រ័យទៅលើល្បឿនសរុប។ ល្បឿនច្រកនីមួយៗស្មើនឹងល្បឿនសរុប ចែកនឹងចំនួនច្រកនៃ Hub។



#### រូបភាពទី២៖ បង្ហាញពីឧបករណ៍ Hub

#### **១.៣.២ ឧទភារសំ** Layer 2 Switch

ដូនកាល Switch ហៅថា Bridge ដែលជាធម្មតាអាចមានត្រឹមតែពីរច្រក។ Switch អាចមាន ច្រើនច្រក(Port) ដែលអាស្រ័យទៅលើថាតើគេត្រូវភ្ជាប់ទៅអង្កត់នៃលែនចំនួនប៉ុន្មាន។ ពេលដុំ ទិន្នន័យមួយមកដល់ច្រកមួយ វាចម្លងទៅត្រឹមតែច្រកគោលដៅមួយប៉ុណ្ណោះ។ ក្នុងករណីខ្លះ វា អាចចម្លងទៅគ្រប់ច្រក កាលណាមេម៉ូរីនៃ Content Address Memory (CAM) របស់វាពេញ។ វា បញ្ចូនទិន្នន័យពឹងផ្អែកលើព័ត៌មាននៅស្រទាប់ទី២នៃម៉ូដែល OSI។ ពោលគឺប្រើអាសយដ្ឋានម៉េក (MAC address) នៃឧបករណ៍ទាំងអស់ដែលភ្ជាប់មកវាសម្រាប់បញ្ចូនទៅគោលដៅ។ ការបញ្ចូន នេះបណ្តាលឱ្យមានដែនផ្សាយធំដូច Hub ដែរ ប៉ុន្តែដែនប៉ះទង្គិចតូច (បើ Switch មានច្រកបញ្ចូន ៤ ដែនប៉ះទង្គិចមានត្រឹមតែ ៤ ដែរ)។ ច្រកនីមួយៗនៃ Switch មានល្បឿនជាក់លាក់ដែល អាស្រ័យទៅលើល្បឿនសរុប។ ល្បឿនច្រកបញ្ចូននីមួយៗស្មើនឹងល្បឿនសរុបនៃ Switch។



#### រូបភាពទី៣៖ បង្ហាញពីឧបករណ៍ Switch

#### **១.៣.៣ ឧចភារេភ៍** Bridge

Bridge ត្រូវគេចាត់ទុកជា Layer 2 Switch។ វាឧបករណ៍ដំណើរការនៅស្រទាប់ទី២នៃម៉ូដែល OSI ហើយគេរៀបចំឡើងដើម្បីភ្ជាប់លែនឬអង្កត់លែន (LAN/LAN Segment) ពីរឬច្រើនចូលគ្នា ដែលនីមួយៗមានដែនប៉ះទង្គិចផ្សេងៗគ្នា ឬ ដើម្បីញែកបណ្តាញមួយទៅជាបណ្តាញច្រើន។ ជា ទូទៅ បណ្តាញទាំងអស់ដែលភ្ជាប់ទៅ Bridge ត្រូវប្រើវិធីការដូចគ្នា ពោលគឺបើប្រើបច្ចេកវិទ្យាលែ ន Ethernet ត្រូវប្រើ Ethernet ទាំងអស់ បើប្រើ AppleTalk ត្រូវប្រើ AppleTalk ទាំងអស់។ មុខងារ ចំបងនៃ Bridge គឺការបញ្ចូនទិន្នន័យ ដោយពឹងផ្អែកលើអាសយដ្ឋានម៉េករបស់ឧបករណ៍បញ្ចូនឬ ទទួល។



រូបភាពទី៤៖ បង្ហាញពីឧបករណ៍ Bridge

ę

#### **9. ຕ. ໔. ຂອສາຄ**ັ້ກ Router

Router ជាប្រភេទឧបករណ៍អន្តរបណ្តាញដែលធ្វើការនៅស្រទាប់ទី៣នៃម៉ូដែល OSI និង ដែលនាំទិន្នន័យផ្សេងៗគ្នាឆ្លងកាត់អន្តរបណ្តាញ ដោយពឹងផ្អែកលើអាសយដ្ឋានអាយភី (IP address) អាសយដ្ឋាន បណ្តាញ (Network address)។ Router អាចសម្រេចស្វែងរកផ្លូវប្រសើរ និងជិតបំផុត សម្រាប់ចែកចាយទិន្នន័យលើបណ្តាញ។ តាមច្បាប់ Router មិនបញ្ជូនដែនផ្សាយពី បណ្តាញមួយទៅបណ្តាញមួយទៀតទេ។ មានន័យថាពេល Switch ឬ Hub បង្កើតដែនផ្សាយ ហើយពេលជួបនឹង Router ដែនផ្សាយទាំងនោះនឹងត្រូវបញ្ចប់។ តែវាក៏ខណ្ឌដែនផ្សាយដែរ។ ចំណែកដែនប៉ះទង្គិចមានលក្ខណៈដូច Switch ដែរ។

សូមចងចាំថា Switch ខណ្ឌដែនប៉ះទង្គិច ចំណែកឯ Router ខណ្ឌដែនផ្សាយៗ



រូបភាពទី៥៖ បង្ហាញពីឧបករណ៍ Routers

#### ១.៣.៥ ទ្រភទណ្តាញ (Gateway)

ច្រកបណ្តាញ (Gateway) ជាឧបករណ៍បំប្លែងវិធីការ (Protocol Converter) និងដំណើរការ នៅស្រទាប់ទី៣នៃម៉ូដែល OSI តែទោះជាយ៉ាងណាក៏ដោយ អាស្រ័យតាមមុខងារ ច្រកបណ្តាញ ក៏ធ្វើការនៅស្រទាប់ផ្សេងៗនៃម៉ូដែល OSI ផងដែរ ដូចជាស្រទាប់ទី៧ ទី ៥ ទី៥។ Router ខ្លួនឯង បំប្លែង ទទួល និង បញ្ជូនបន្តដុំទិន្នន័យកាត់ត្រឹមតែបណ្តាញដែលប្រើវិធីការដូចគ្នា។ ផ្ទុយមកវិញ ច្រកបណ្តាញអាចទទួលយកដុំទិន្នន័យពីវិធីការមួយ និងបំប្លែងវាទៅជាដុំទិន្នន័យសម្រាប់វិធីការ មួយផ្សេងទៀត មុននឹងរុញចេញ។ ច្រកបណ្តាញគឺជា Router។



#### រូបភាពទី៦៖ បង្ហាញពីឧបករណ៍ Gateway

#### ១.៣.៦ ចំណុខឆេតអំសេស/ឆេអំសេសន័ញ (Access Point/Wireless AP)

ចំណុចអាក់សេសឬអាក់សេសភ័ញគឺជាឧបករណ៍ដែលធ្វើការជាពួរ (core) នៃបណ្តាញឥត ខ្សែ សម្រាប់ភ្ជាប់ឧបករណ៍វ៉ាយហ្វាយទៅបណ្តាញកុំព្យូទ័រ។



#### រូបភាពទី៧៖ បង្ហាញពីឧបករណ៍ Wireless Access Point

#### 9.៤. ភារតារចារចណ្តាញ (Network Defense)

ការប្រើប្រាស់ឧបករណ៍និងដំណោះស្រាយដ៍ត្រឹមត្រូវអាចជួយការពារបណ្តាញរបស់យើង បានប្រសើរ។ ឧបករណ៍ការពារបណ្តាញមានច្រើនប្រភេទ និងអាចការពារតាមតូនាទីរបស់វា។ យើងអាចប្រើឧបករណ៍ទាំងនេះជាខ្សែការពារទី១ ទី២ ទី៣ ទី៤ និងខ្សែការពារចុងក្រោយ នៃ បណ្តាញកុំព្យូទ័ររបស់យើង។ យ៉ាងតិចណាស់ យើងត្រូវរៀបចំខ្សែការពារជាច្រើនចូលគ្នា ផ្ទុយ មកវិញ មានខ្សែការពារបណ្តាញតែមួយ មិនអាចការពារបណ្តាញបានទេ។

### **១.៤.១ ຬញុភំខេះ**ឆ្លីខ (Firewall)

ជញ្ចាំងភ្លើងគឺជាប្រព័ន្ធសុវត្ថិភាព (ហាដវែរឬសុសវែរ) ដែលគ្រួតពិនិត្យលំហូរទិន្នន័យពីកុំព្យូ ទ័រមួយទៅកុំព្យូទ័រមួយទៀត ឬពីបណ្តាញកុំព្យូទ័រមួយទៅបណ្តាញកុំព្យូទ័រមួយទៀតឬពីអ៊ីនធឺណិ ត ប្រឆាំងនឹងអាក់សេសខុសច្បាប់ពីខាងក្រៅ ឬ ប្រឆាំងនឹងការខ្វួចហាដវែរនៅកន្លែងណាមួយនៃ បណ្តាញ។ គោលបំណងសំខាន់នៃជញ្ជាំងភ្លើងគឺបិទចរាចរទិន្នន័យពីខាងក្រៅ ប៉ុន្តែក៏អាចបិទ ចរាចរទិន្នន័យពីខាងក្នុងបានដែរ។ ជញ្ជាំងភ្លើងគឺបិទចរាចរទិន្នន័យពីខាងក្រៅ ប៉ុន្តែក៏អាចបិទ ចរាចរទិន្នន័យពីខាងក្នុងបានដែរ។ ជញ្ជាំងភ្លើងជាយន្តការការពារជូរមុខទីមួយប្រឆាំងនឹងល្មួច ណាមួយ។ ជញ្ជាំងភ្លើងអាចជាហាដវែរដែលសង់នៅក្នុងឧបករណ៍ដូចជា Router ដែលត្រូវការ រៀបចំបន្តិចបន្តួចបន្ថែមទៀតដើម្បីឱ្យមានប្រសិទ្ធភាព និង ដែលប្រើបច្ចេកទេស Packet-Filter។ ហើយវាក៏អាចជាសុសវែរពេញនិយមបំផុតដែលអាចការពារបណ្តាញសម្រាប់អ្នកប្រើប្រាស់តាម ផ្ទះ ដែលអាចប្រឆាំងនឹងមេរាគផងដែរ និង ដែលត្រូវការអាប់ដេតជាប្រចាំ។ ជញ្ជាំងភ្លើងអាចជាប ន្សំទាំងពីរប្រភេទចូលគ្នា ហើយជញ្ជាំងភ្លើងតាំងនៅចន្លោះបណ្តាញខាងក្នុង ដូចជា សែន លែន មែន ឬ វែន និង បណ្តាញខាងក្រៅ ដូចជាអុីនធឺណិត ដើម្បីការពារបណ្តាញខាងក្នុង។



រូបភាពទី៨៖ បង្ហាញពីជញ្ជាំងភ្លើងឬ Firewall



រូបភាពទី៩៖ បង្ហាញពីការតប្រព័ន្ធបណ្តាញ

#### ១.៤.២ ទ្រព័ន្ធអន្តេតល្មួច (Intrusion Detection System)

ប្រព័ន្ធអង្កេតល្មួចគឺជាហាដវែរឬសុសវែរមួយប្រភេទដែលរចនាឡើងសម្រាប់ប្រមូលផ្តុំ អង្កេត វិភាគព័ត៌មាន និង ត្រូតពិនិត្យរាល់សកម្មភាពក្នុងកុំព្យូទ័រឬបណ្តាញកុំព្យូទ័រ ដើម្បីកំណត់អត្ត សញ្ញាណរង្វាយប្រហារឬសកម្មភាពល្ងច ក្នុងគោលបំណងការពារ ភាពសម្ងាត់(Confidentiality) សុក្រឹតភាព(Integrity) លទ្ធភាព (Availability) និង គណនេយ្យភាព(Accountability)។

បច្ចុប្បន្ន មានបច្ចេកវិទ្យាថ្មីមួយទៀតដែលអាចចាត់ទុកថាជាបច្ចេកវិទ្យាជំនាន់ទី២នៃប្រព័ន្ធ អង្កេតល្មួចគឺ ប្រព័ន្ធអង្កេតវិវាទ(Breach Detection System)។

ប្រព័ន្ធអង្កេតវិវាធគឺជាហាដវែរឬសុសវែរមួយប្រភេទដែលរចនាឡើងសម្រាប់អង្កេត និង ត្រូត ពិនិត្យ សកម្មភាពម៉ាល់វែរ កិច្ចកំហែងផ្សេងៗ ក្រោយពេលមានវិវាទកើតឡើងក្នុងកុំព្យូទ័រឬ បណ្តាញកុំព្យូទ័រ។ សាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច



រូបភាពទី១០៖ បង្ហាញពីការរៀបចំប្រព័ន្ធដើម្បើអង្កេតពីការជ្រៀតចូលនៃ Viruses

១.៤.៣ ទ្រព័ន្ធទទ្ធារឈ្នួទ (Intrusion Prevention System)

ប្រព័ន្ធបង្ការល្មួចគឺជាហាដវែរឬសុសវែរមួយប្រភេទដែលរចនាឡើងសម្រាប់អង្កេត បង្ការ គ្រូតពិនិត្យអាក់សេសឬសកម្មភាពក្នុងកុំព្យូទ័រឬបណ្តាញកុំព្យូទ័រ និង ចាត់វិធានឆុតកាល (realtime) ទៅនឹងសកម្មភាពនោះ ដើម្បីការពាររង្វាយប្រហារ ការបំពាន ឬ សកម្មភាពល្ងច។ ជាទូទៅ គេប្រើប្រាស់វាជាមួយប្រព័ន្ធអង្កេតល្មួច។

ដូចគ្នាទៅនឹងប្រព័ន្ធអង្កេតល្មួចដែរ មានបច្ចេកវិទ្យាចុងក្រោយដែលជាបច្ចេកវិទ្យាជំនាន់ទី២ នៃប្រព័ន្ធបង្ការល្មួចគឺប្រព័ន្ធបង្ការវិវាទ (Breach Prevention System)។

ប្រព័ន្ធបង្ការវិវាទគឺជាហាដវែរឬសុសវែរមួយប្រភេទដែលរចនាឡើងសម្រាប់អង្កេត បង្ការ វិភាគសកម្មភាពម៉ាល់វែរ កិច្ចកំហែងផ្សេងៗ និង ចាត់វិធានការឆុតកាល (real-time) មុនពេលវិវាទ កើតឡើងក្នុងកុំព្យូទ័រឬបណ្តាញកុំព្យូទ័រ។

បរិញ្ញាបត្រសេដ្ឋកិច្ចព័ត៌មានវិទ្យា

សាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច



#### រូបភាពទី១១៖ បង្ហាញពីការរៀបចំប្រព័ន្ធដើម្បើបង្ការពីការជ្រៀតចូលនៃ Viruses

9.៤.៤ ទ្រព័ន្ធន្រូនគេរាក់សេសបណ្ដាញ គឺជាបច្ចេកវិទ្យា វិធីសាស្ត្រ ឬ ដំណោះស្រាយដែលអនុវត្ត ប្រព័ន្ធត្រូតអាក់សេសបណ្ដាញ គឺជាបច្ចេកវិទ្យា វិធីសាស្ត្រ ឬ ដំណោះស្រាយដែលអនុវត្ត ដោយបង្ខំនូវគោលនយោបាយសន្តិសុខប្រព័ន្ធព័ត៌មានសម្រាប់កំណត់ បែងចែក ចាត់ចែងសិទ្ធិ គ្រប់គ្រង ដោយស្វ័យប្រវត្តលើឧបករណ៍ទាំងអស់ដែលចូលអាក់សេសបណ្ដាញ ដើម្បីធានា បង្កើននិងដំរុញ ការពារសន្តិសុខបណ្ដាញ ហើយនិង កាត់បន្ថយហានិភ័យ។

#### សាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច

#### បរិញ្ញាបត្រសេដ្ឋកិច្ចព័ត៌មានវិទ្យា



#### រូបភាពទី១២៖ បង្ហាញពីប្រព័ន្ធ Network Access Control System

#### **9.໔.໕ ອະງຸຣະເຣອອ** (Web Filter)

ចម្រោះវេបជាបច្ចេកវិទ្យា កម្មវិធី ឬលក្ខណៈមួយដែលអាចរេងទំព័រវេបឬខ្លឹមសារនៃទំព័រវេប អំឡុងពេលប្រើប្រាស់ធ្វើអាក់សេសទំព័រវេប។

#### **9.໔.៦ ເសຮູບສະເຄ**ັ້ລ Proxy (Proxy Server)

សេវូបករណ៍ Proxy ជាសេវូបករណ៍ទាំងឡាយណាដែលដើរតូជាអន្តរការីចំពោះសំណើរបស់ អតិថ្វបករណ៍ទៅសេវូបករណ៍ពិត សម្រាប់សេវាឬធនធាន។ មានសេវូបករណ៍ Proxy ជាច្រើន ប្រភេទដែលអាចប្រើបានអាស្រ័យលើគោលបំណងផ្សេងៗ។ សេវូបករណ៍ Proxy អាចការពារ បានត្រឹមតែកម្មវិធីទាំងឡាយណាដែលគាំទ្រវា។

#### ១.៤.៧ អទនិទាល់ទេ៖ (Anti-malware)

វាជាសុសវែរម្យ៉ាងដែលបង្កើតឡើងដើម្បីប្រឆាំង រារាំង ការពារ អង្កេត និងលុបបំបាត់ម៉ាល់វែ រនៅក្នុងកុំព្យូទ័រ ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ឬ ឧបករណ៍កុំព្យូធីង(Computing devices)។ ម៉ាល់វែរ ជាសុសវែរឬក្ខដសុសវែរ ដែលបង្កើតឡើងក្នុងគោលបំណងមិនល្អណាមួយនិងមានសមត្ថភាព បំផ្លាញឯកសារប្រព័ន្ធកុំព្យូទ័រ ...។ ឧ. មេរោគកុំព្យូទ័រជាកម្មវិធីប្រភេទម៉ាល់វែរ។

#### ១.៥ ទ្រនោនអគ្គត់ទណ្ណាញ (Network Segment Types)

អង្កត់បណ្តាញគឺជាផ្នែកមួយនៃបណ្តាញកុំព្យូទ័រដែលត្រូវបានបំបែកចេញពីបណ្តាញមួយ ដោយឧបករណ៍ដូចជា Hub, Bridge, Switch និង Router ។ ផ្នែកនីមួយៗអាចមានកុំព្យូទ័រមួយឬ ច្រើនឬឧបករណ៍ផ្សេងទៀត។



រូបភាពទី១៣៖ បង្ហាញពី Network Segment Types

#### 

បណ្តាញសាធារណៈគឺជាបណ្តាញមួយប្រភេទ ដែលជនទូទៅអាចចូលប្រើបាន និង អាច ភ្ជាប់ទៅបណ្តាញផ្សេងទៀតឬអុីនធឺរណិត។ បណ្តាញនេះផ្ទុយពីបណ្តាញឯកជនដែលការរឹត បន្តឹងនិងច្បាប់ប្រើប្រាស់ ត្រូវបានបង្កើតឡើងដើម្បីកាត់បន្ថយការចូលប្រើ។ ពេលធ្វើការអាក់ សេសបណ្តាញសាធារណៈ អ្នកប្រើប្រាស់ត្រូវស្វ័យប្រុងប្រយ័ន្នចំពោះហានិភ័យ។

#### ទ.៥.២ ទន្ទោញឯកខន (Private Network)

បណ្តាញឯកជនគឺជាបណ្តាញកុំព្យូទ័រមួយដែលប្រើអាសយដ្ឋានអាយភីឯកជន (private IP address)។ ស្តិច (Specification)ទាំង IPv4 និង IPv6 បានកំណត់នូវប្រវែងអាសយដ្ឋានអាយភី ឯកជន។ អាសយដ្ឋានទាំងនេះត្រូវបានប្រើជាទូទៅសម្រាប់បណ្តាញក្នុងតំបន់ (លែន) នៅក្នុង តំបន់លំនៅដ្ឋាន ការិយាល័យ និង សហគ្រាស។ បណ្តាញឯកជនមានការរឹតបន្តឹងនិងច្បាប់ប្រើ ប្រាស់ដើម្បីកាត់បន្ថយការចូលប្រើ ហានិភ័យលើសន្តិសុខ។

#### ១.៥.៣ ខណ្ដាញតូនភាត់ (semi-public Network)

បណ្តាញសាធារណៈនិងបណ្តាញឯកជនផ្តុំចូលគ្នាបង្កើតបានជាបណ្តាញពាក់កណ្តាលសា ធារណៈ។ ជាធម្មតា វាជាបណ្តាញដែលអ្នកប្រើប្រាស់អាចធ្វើការអាក់សេសទៅបណ្តាញសាធារ ណៈ។

#### 9.៥.៤. ចណ្តាញតំមន់ស (Demilitarized Zone-DMZ)

បណ្តាញតំបន់សជាបណ្តាញរងមួយរបស់ស្ថាប័នសម្រាប់ភ្ជាប់កុំព្យូទ័រឬឧបករណ៍ (host) ដែលត្រូវការអាក់សេសទៅបណ្តាញខាងក្រៅ ពោលគឺទៅអុីនធឺណិត ឧទាហរណ៍៖ សេវូបករ ណ៍វេប (Web servers)។ DMZ អាចជាបណ្តាញសមស្របសម្រាប់ដោះស្រាយជាមួយរង្វាយ ប្រហារខាងក្រៅ ហើយអាចត្រូវបានប្រើដើម្បីអនុវត្តគោលនយោបាយគ្រប់គ្រងអ្នកប្រើខាង ក្នុង ប៉ុន្តែមានការប្រើតិចត្ចចប្រឆាំងនឹងរង្វាយប្រហារខាងក្នុង។

# **ඵ්**ශු**ඝ**ଛි්ප

# ផែនភារអនុទត្តនំគម្រេាខ

ផែនការសកម្មភាពជាចំណុចសំខាន់នៃការសម្រេចគម្រោង។ ខាងក្រោមជាផែនការអនុវត្តន៍ នៃគម្រោងនៃប្រព័ន្ធបណ្តាញណែតវ៉ីក។

## ព្រ ៦ ឧរួលាតាខំនេះទ្រង់សេខ

ដើម្បីបង្កើតប្រព័ន្ធនៃការសិក្សាស្រាវជ្រាវនេះឱ្យទទួលបានជោគជ័យតាមការរំពឹងទុក អ្នក អនុវត្តគម្រោងត្រូវរៀបចំវិធីសាស្ត្រឱ្យបានច្បាស់លាស់ ដូចខាងក្រោមជាដំណាក់កាលនៃការ រៀបចំ៖

ទី១៖ កំណត់បញ្ហានិងគោលបំណង

ទី២៖ ប្រមូលព័ត៌មាននិងឯកសារសម្រាប់តម្រូវការគរម្រាង

ទី៣៖ វិភាគតម្រវការប្រព័ន្ធ និង រៀបចំរចនាប្រព័ន្ធ

ទី៤៖ ដំឡើង បង្គុំ និងពិសោធ

ទី៥៖ រៀបចំនិងក្រាងឯកសារ

# ២.២ ផែនភារកាលទីភាគនិចភារកិច្ច

ខាងក្រោមជាបំណែងចែកពេលវេលានិងភារកិច្ចអ្នកទទួលខុសត្រូវ។

ល.រ	ផែនការ	ពេលវេលា	ភារកិច្ច
១	កំណត់ពីបញ្ហានិងគោលបំណង	២សប្តាហ៍	គង់ រក្សា សន សំខាន់
Ե	ប្រមូលព័ត៌មានឯកសារសម្រាប់តម្រវការ	២សប្តាហ៍	គង់ រក្សា សន សំខាន់
	គឺម្រោង		
៣	វិភាគតម្រវការប្រព័ន្ធ និង រៀបចំរចនាប្រព័ន្ធ	២សប្តាហ៍	គង់ រក្សា សន សំខាន់
લ	ដំឡើង បង្គុំ និងពិសោធ	២សប្តាហ៍	គង់រក្សា សន សំខាន់
ະ	រៀបចំនិងក្រងឯកសារ	៣សប្តាហ៍	គង់ រក្សា សន សំខាន់

#### ២.៣ លក្ខខណ្ឌតិចតម្រូខភារសម្ភារ: (Security Testing)

គម្រោងនៃការរៀបចំប្រព័ន្ធនេះត្រូវការសម្ភារៈនិងលក្ខខណ្ឌមួយចំនួន។លក្ខខណ្ឌនិងសម្ភារៈ ទាំងនៅរួមមាន៖

- Router: TP-LINK Wireless N Router TL-WR940N
- Wireless Access Point: TP-LINK Wireless N Router TL-WR940N
- កុំព្យូទ័រ៖ CPU: Core i7 8Gen, RAM: 8GB , SSD: 500GB, Graphic Card: GTX-1050 TI 4GB, HDD: 1TB,
- កម្មវិធី: Nmap, Nessus,

#### ២-៤. លន្តផលរំពីខនុត

ក្នុងពេលការសិក្សាពីគម្រោង ក្រុមរបស់ពួកយើងបានរំពឹងទុកចំនួនពីលទ្ធផលចំនួន ៣ធំៗ៖ ១.ពួកយើងរំពឹងទុកថាវាអាចជួយ ការពារប្រព័ន្ធបណ្តាញរបស់អ្នកពីការជ្រៀតចូលនៃ Virus នឹងងាយស្រួលក្នុងការគ្រប់គ្រង

២.ការពង្រឹងទៅលើសន្តិសុខរបស់ Wireless Router ដូចជាការបើកដំណើរការ Firewall, Web Filter and Access Control

៣. ការពារទៅលើ End-Devices ដែលប្រើប្រាស់ដើម្បី Access ចូលទៅកាន់ Router ដូចជា ការប្រើប្រាស់កម្មវិធីជំនួយ នឹងបើកដំណើរការប្រព័ន្ធសន្តិសុខដែលមានស្រាប់នៅលើវា

# ຬំពូភនី៣ ಜំន្បើទតិទទទ្ទុំសត្តិសុខមណ្តាញ

ជំពូកនេះ យើងបរិយាយអំពីវិធីសាស្ត្រនៃការសិក្សាស្រាវជ្រាវ។ វិធីសាស្ត្រស្រាវជ្រាវ របស់យើងគឺដំឡើងនិងបង្គុំសន្តិសុខបណ្តាញកុំព្យូទ័រកម្រិតតូចដែលមានរចនាសម្ព័ន្ធដូច ខាងក្រោម៖



រូបភាពទី ១៤ ៖ បង្ហាញពីដ្យាក្រាមនៃបណ្តាញសន្តិសុខ Network

**ព.១ សន្តិសុខមន្តភាញ** (Network Security)

## ព.១.១ ទេៀមនៃគារដំណើរ៩ញាំខន្លើទ (Firewall)

ដើម្បីឲ្យណែតវ៉ឹកយើងមានសុវត្ថិភាពយើងត្រូវ តំឡើងជញ្ជាំងភ្លើង នឹងកំណត់ជញ្ជាំងភ្លើង ដូចខាងក្រោម៖

១.ចូលទៅកាន់ Console Screen របស់ Router ហើយរកមើលពាក្យឋា Security-> Basic Security អ្នកនឹងបានឃើញ ពាក្យឋា Firewall ចុច ពាក្យឋា Enable ហើយចុច Save៖ ២.បន្ទាប់ពីចុច Enable Firewall រួចហើយ សូមចូលទៅកាន់ពាក្យថា Advanced Security -> Enable Dos Protection-> ចុច check នៅត្រង់ Ignore Ping Packet from WAN Port to Router->Save៖

tp-link			
Ola la construction de la constr			
Status			
Quick Setup			
WPS	Advanced Security		
Working Mode			
Network	Packets Statistics Interval (5 ~ 60):	10 V Seconds	
Wireless			
Guest Network	DoS Protection:	Disable      Enable	
DHCP			
Forwarding	Enable ICMP-FLOOD Attack Filtering		
Security	ICMP-FLOOD Packets Threshold (5 ~ 3600)	50 Parkets/Secs	
- Basic Security			
- Advanced Security	Easthia LIDB ELOOD Ethnica		
- Local Management	Enable ODF-FLOOD Filtering	E00 Beskele Bess	
- Remote Management	UDP-FLOOD Packets Threshold (5 ~ 3600):	500 Packets/Secs	
Parental Control			
Access Control	Enable TCP-SYN-FLOOD Attack Filtering		
Advanced Routing	TCP-SYN-FLOOD Packets Threshold (5 ~ 3600):	50 Packets/Secs	
Bandwidth Control			
IP & MAC Binding	Ignore Ping Packet from WAN Port to Router		
Dynamic DNS	Forbid Ping Packet from LAN Port to Router		
IPv6 Support			
System Tools	Save Blocked DoS Host Li	ist	
Logout			

#### រូបភាពទី ១៥ ៖ បង្ហាញពីការបើក Firewall

៣.បន្ទាប់មកចូលទៅកាន់ Local Management ជ្រើសរើសយក Only ហើយចុចពាក្យឋា Add អ្នក នឹងបានឃើញ Mac Address បង្ហាញឡើង បន្ទាប់មក Save៖

Status	
Quick Setup	
WPS	Local Management
Working Mode	
Network	Management Rules
Wireless	
Guest Network	<ul> <li>All the PCs on the LAN are allowed to access the Router's Web-Based Utility</li> </ul>
DHCP	Only the PCs listed can browse the built-in web pages to perform Administrator tasks
Forwarding	MAC 1: 0C-9D-92-57-1D-5B
Security	MAC 2:
- Basic Security	MAC 3:
- Advanced Security	MAC 4
- Local Management	
- Remote Management	Your PC's MAC Address: UC-9D-92-57-10-58 Add
Parental Control	
Access Control	Save
Advanced Routing	
Bandwidth Control	
IP & MAC Binding	
Dynamic DNS	
IPv6 Support	
System Tools	
Logout	

រូបភាពទី ១៦ ៖ បង្ហាញពីការការកំណត់ទៅលើ Local Management លើ Firewall

៤.បន្ទាប់មកចូលទៅកាន់ Access Control ចុចពាក្យឋា Deny ហើយចុច Save៖

	450M Wireless N Router Model No. TL-WR940N
Status	
Quick Setup	
WPS	Access Control Rule Management
Working Mode	
Network	Enable Internet Access Control
Wireless	
Guest Network	Default Filter Policy
DHCP	Allow the parkets specified by any enabled access control policy to pass through the Router
Forwarding	Deput the previous spectrum any any answer assess sector pointy to pace through the Router
Security	Deny are packets specified by any enamed access control porcy to pass in dogin the Noticel
Parental Control	Save
Access Control	
- Rule	ID Rule Name Host Target Schedule Status Modify
- Host	Setup Wizard
- Target	
- Schedule	Add New Enable All Disable All Delete All
Advanced Routing	
Bandwidth Control	Move ID To ID
IP & MAC Binding	
Dynamic DNS	Previous Next Current No. 1 Y Page
IPv6 Support	
System Tools	
Logout	

រូបភាពទី ១៧ ៖ បង្ហាញពីការបើកដំណើរការលើ Access Control

៥.ចូលមកកាន់ Host -> Add New -> ទៅ Copy Mac Address ពី Local Management ហើយ បន្ទាប់មកយើងចុច Save៖

tp-link	Model No. TL-WR940N			
Status				
Quick Setup				
WPS	Host Settings			
Working Mode				
Network	ID Host Description	Information		Modify
Wireless	Add New Delete All			
Guest Network				
DHCP		Drovioue Mi	Current No. 1 +- Dans	
Forwarding			Current No. 1 V Page	
Security				
Parental Control				
Access Control				
- Rule				
- Host				
- Target				
- Schedule				
Advanced Routing				
Bandwidth Control				
IP & MAC Binding				
Dynamic DNS				
IPv6 Support				
System Tools				
A second s				

រូបភាពទី ១៨ ៖ បង្ហាញពីការ Add New Host នៅលើ Access Control

#### បរិញ្ញាបត្រសេដ្ឋកិច្ចព័ត៌មានវិទ្យា

#### សាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច

tp-link	Model No. TL-WR940N	
Status		
Quick Setup	Add or Modify a Host Entry	
WPS	Add of Modily a Host Entry	
Working Mode		
Network	Mode:	MAC Address V
Wireless	Host Description:	
Guest Network	MAC Address:	0C-9D-92-57-1D-5E
DHCP		
Forwarding		
Security		Save Back
Parental Control		
Access Control		
- Rule		
- Host		
- Target		
- Schedule		
Advanced Routing		
Bandwidth Control		
IP & MAC Binding		
Dynamic DNS		
IPv6 Support		
System Tools		
A		

#### រូបភាពទី ១៩ ៖ បង្ហាញពី Mac Address នៅលើ Access Control

៦.ចូលមកកាន់ Target ហើយបំពេញពំត័មានដែលមាន ដូចខាងក្រោម ហើយបន្ទាប់មក ចុច

	450M Wireless N Router Model No. TL-WR940N	
Status		
Quick Setup		
WPS	Add or Modify an Access Targe	at Entry
Working Mode		
Network	Mode:	Domain Name 🗸
Wireless	Target Description;	yahoo
Guest Network	Domain Name:	www.vahoo.com
DHCP		
Forwarding		
Security		
Parental Control		
Access Control		
- Rule		Save Back
- Host		
- Target		
- Schedule		
Advanced Routing		
Bandwidth Control		
IP & MAC Binding		
Dynamic DNS		
IPv6 Support		
System Tools		
Logout		

#### រូបភាពទី ២០ ៖ បង្ហាញពីការកណត់ទៅលើ Target នៅលើ Access Control

Save

៧.បន្ទាប់មកចូលមកកាន់ Schedule ហើយធ្វើការបំពេញពំត័មានដូចខាងក្រោម ហើយសូមចុច

	450M Wireless N Router Model No. TL-WR940N	
Status		
Quick Setup		
WPS	Advance Schedule Settings	
Working Mode		
Network	Note: The Schedule is based on the time of the Router.	
Wireless		
Guest Network		
DHCP	Schedule Description: Valido	
Forwarding	Day: 🔿 Everyday 💿 Select Days	
Security	🗹 Mon 🗹 Tue 🗹 Wed 🗹 Thu 🗹 Fri 🗌 Sat 🗌 Sun	
Parental Control	Time: all day-24 hours:	
Access Control	Start Time: 1200 (HHMM)	
- Rule	Stop Time: 1400 (HHMM)	
- Host		
- Target		
- Schedule	Save Back	
Advanced Routing		
Bandwidth Control		
IP & MAC Binding		
Dynamic DNS		
IPv6 Support		
System Tools		
Logout		
1. Sec.		

#### រូបភាពទី ២១ ៖ បង្ហាញពីការកំណត់ Schedule នៅលើ Acess Control

៨.ចូលមកកាន់ Rule ហើយចុចតាមដូចរូបខាងក្រោមដែលបានបង្ហាញ ហើយចុច Save បន្ទាប់ មកចូលទៅកាន់ Add New នឹងបំពេញពិត័មានដូចនៅក្នុងរូបដែលបានបង្ហាញនៅផ្ទាំងទីពីរ៖

Status		
Quick Setup		
WPS	Access Control Rule Management	
Working Mode		
Network	Enable Internet Access Control	
Wireless		
Guest Network	Default Filter Policy	
DHCP	Allow the packets specified by any enabled access control policy to pass through the Router	
Forwarding	Denu the parkets specified by any enabled access control policy to pass through the Router	
Security	Unerry the parveces specimen by any ensured access control pointy to pass through the House	
Parental Control	Save	
Access Control		
- Rule	ID Rule Name Host Target Schedule Status Modify	
- Host	Setup Wizard	
- Target		
- Schedule	Add New Enable All Disable All Delete All	
Advanced Routing		
Bandwidth Control	Move ID To ID	
IP & MAC Binding		
Dynamic DNS	Previous Next Current No. 1 V Page	
Pv6 Support		
System Tools		

#### រូបភាពទី ២២ ៖ បង្ហាញពីការកំណត់ Rule នៅលើ Access Control
រូបភាពទី ២៣ ៖ បង្ហាញពីការ Add New Rule នៅលើ Access Control

៩.ចំណុចចុងក្រោយអ្នកនឹងបានឃើញ ទម្រង់បែបនេះដូចក្នុងរូបខាងក្រោម៖

	450M Wireless N Router Model No. TL-WR940N
Status	
Quick Setup	
WPS	Access Control Rule Management
Working Mode	
Network	Enable Internet Access Control
Wireless	
Guest Network	Default Filter Policy
DHCP	Allow the packets specified by any enabled access control policy to pass through the Router
Forwarding	Deriv the narkets sharified by any enabled arease control notice to hase through the Reuter
Security	Outry the packets specified by any enabled access control pointy to pass introduct the reduct
Parental Control	2944
Access Control	
- Rule	ID Rule Name Host Target Schedule Status Modify
- Host	1 Router Firewall <u>myComputer yahoo yahoo</u> 🗹 Edit Delete
- Target	Setup Wizard
- Schedule	
Advanced Routing	Add New Enable All Disable All Delete All
Bandwidth Control	
IP & MAC Binding	Move ID To ID
Dynamic DNS	
IPv6 Support	Previous Next Current No. 1 V Page
System Tools	
Logout	

រូបភាពទី ២៤ ៖ បង្ហាញពីដំណាក់កាលចុងក្រោយពេលដំឡើងរួច

ការបើកអោយដំណើរការរបស់ Firewall នៅលើ Wireless Router ត្រូវបានដំណើរការដូច ទៅតាមការរៀបរាប់នៅខាងលើ៕

## **៣.១.២ ៖ខៀមនៃការដំនៀ្មច ទេម ទៀលឆើ** (Web Filter)

យើងដឹងហើយថា Web Filter មានសារ:សំខាន់ណាស់ក្នុងការចូលរូមជាមួយការតំឡើងនៃ ណែតវ៉ឹក។ ដូចនេះយើងគូរតែដំឡើង Web Filter តាមលំនាំខាងក្រោម៖

១. ដំបូងអ្នកត្រូវបើកវេបប្រោវស្វើ ( Web Browser) នឹងចូលក្នុងប្រភេទវោតទ័ររបស់យើង



## រូបភាពទី ២៥ ៖ បង្ហាញអំពីការចូលក្នុងពាតទ័រតាម Web Browser

២. អ្នកត្រូវតែចូលទៅក្នុង Username នឹង លេខសម្ងាត់របស់អ្នក នៅក្នុង រោតទ័ររបស់អ្នក

LOGIN	
Login to the router :	
User N	ime : Admin
Passw	ord : Login

## រូបភាពទី ២៦ ៖ បង្ហាញអំពីការវាយឈ្មោះអ្នកប្រើប្រាស់នឹងលេខសម្ងាត់

៣. បន្ទាប់ពីអ្នកចូលទៅក្នុងរោតទ័ររួចហើយ រួចត្រូវស្វែងរក ពាក្យ Advanced Tab បន្ទាប់បក ស្វែងរកពាក្យ Website Filter។ ជ្រើសរើសជម្រើស Deny Computer Access to ONLY these site បន្ទាប់វាយ URL ដែលអ្នកចង់បិទមិនអនុញ្ញាត ។បន្ទាប់មកចុចពាក្យ Save Setting ។



រូបភាពទី ២៧ ៖ បង្ហាញអំពីការជ្រើសរើសនូវច្បាប់ Website Filter

៥. បន្ទាប់អ្នកត្រូវចូលទៅក្នុង Access Control រួចចុចលើ ជ្រើស នៅក្នុង Enable Access Control បន្ទាប់មកចុចលើពាក្យ Add Policy

//	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
VIRTUAL SERVER	ACCESS CONTROL				Helpful Hints
PORT FORWARDING	The Access Control op	tion allows you to control	access in and out of your	network. Use this	Check Enable
APPLICATION RULES	feature as Access Cont	rols to only grant access to	to approved sites, limit we	b access based on	Access Control if you want to enforce rules
	Save Settings Don't	t Save Settings	ppicacions inte r 2r a cilicies	or games.	that limit Internet access from specific LAN computers.
ACCESS CONTROL	ACCESS CONTROL				<ul> <li>Click Add Policy to start the processes of</li> </ul>
WEBSITE FILTER	Enable Acces	s Control : 🔟 🥢			creating a rule. You can cancel the process at any
INBOUND FILTER			1		time. When you are finished creating a rule it
FIREWALL SETTINGS		Add Policy			will be added to the
ROUTING					Click the Edit icon to
ADVANCED WIRELESS	POLICY TABLE				modify an existing rule using the Policy Wizard.
WI-FI PROTECTED SETUP	Enable Policy	Machine Fi	Itering Logged	Schedule	Click the Delete icon to permanently remove a
ADVANCED NETWORK	Save Settings Don't	Save Settings			rule.
GUEST ZONE					
IPV6 FIREWALL					
IPV6 ROUTING					

## រូបភាពទី ២៨៖ បង្ហាញអំពីការជ្រើសរើសនូវ Access Control

៥. ចុចពាក្យ Next នៅក្នុង Add New Policy

	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
VIRTUAL SERVER	ADD NEW POLICY				
PORT FORWARDING	hoonen rocier				
APPLICATION RULES	This wizard will guid	e you through the folk	owing steps to add a ne	w policy for Access Co	ntrol.
QOS ENGINE	Step 1 - Choose a uniq	ue name for your policy			
NETWORK FILTER	Step 2 - Select a sche	dule			
ACCESS CONTROL	Step 3 - Select the ma	chine to which this policy	applies		
WEBSITE FILTER		in the contract card pointy	appilos		
INBOUND FILTER	Step 4 - Select filtering	method			
FIREWALL SETTINGS	Step 5 - Select filters				
ROUTING	Step 6 - Configure We	b Access Logging			
ADVANCED WIRELESS					
WI-FI PROTECTED SETUP		Prev	Next Save C	ancel	
ADVANCED NETWORK			-		
GUEST ZONE					

## រូបភាពទី ២៩ ៖ បង្ហាញអំពីការចុចពាក្យ Next នៅលើ Add New Policy

៦. បន្ទាប់មកអ្នកត្រូវវាយពាក្យ Website Filter នៅក្នុង Policy Name រួចចុចលើពាក្យ Next



រូបភាពទី ៣០ ៖ បង្ហាញអំពីការវាយពាក្យ Website Filter ក្នុង Policy Name

៧. រូចមកអ្នកត្រូវ Selected Always នឹងវាយពាក្យ Always នៅក្នុង Details រួចចុចពាក្យបន្ទាប់



## រូបភាពទី ៣១ ៖ បង្ហាញអំពីការវាយពាក្យ Always នឹង ជ្រើសរើស Always

៨. ជ្រើសរើសនូវប្រភេទម៉ាស៊ីនដែលអ្នកចង់ដាក់នៅក្នុង Address Type , IP Address រូចចុច ពាក្យ OK បន្ទាប់មកជ្រើសរើសពាក្យ Next

Select the machine to which the	this policy applies.	
Specify a machine with its IP or MAC have a policy. Address Type: () IP	AC address, or select "Other Machines" for machines that do	not
IP Address: 192.168.0	3.0.100 << 07505NBWIN7 (192.168.0.100) -	
Machine Address:	<< Computer Name v	
	Copy Your PC's MAC Address	
Machine		
	Prev Next Save Cancel	

រូបភាពទី ៣២ ៖ បង្ហាញអំពីការវាយ Address Type នឹង IP Address

៩. ជ្រើសរើសពាក្យ Block Some Access ក្នុង Method ព្រមទាំង ចុច ជ្រើស ក្នុង Apply Web Filter រួចចុចលើពាក្យ Next



### រូបភាពទី ៣៣ ៖ បង្ហាញអំពីការជ្រើសរើសយក Apply Web Filter

## ១០. បន្ទាប់មកអ្នកត្រូវត្រៃជ្រើសរើសរវាង Disable នឹង Enable

	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
VIRTUAL SERVER	STEP 6: CONFIGURE W	FR ACCESS LOGGING			
PORT FORWARDING	STEP 0. CONTROLE I	COMING			
APPLICATION RULES	W	eb Access Logging : @	Disabled		
QOS ENGINE		0	Enabled		
NETWORK FILTER					
ACCESS CONTROL		Prev	Next Save C	ancel	
WEBSITE FILTER			a constant		
INBOUND FILTER					
FIREWALL SETTINGS					
ROUTING					
ADVANCED WIRELESS					
WI-FI PROTECTED SETUP					
ADVANCED NETWORK					
GUEST ZONE					
IPV6 FIREWALL					
IPV6 ROUTING					

### រូបភាពទី ៣៤ ៖ បង្ហាញអំពីការជ្រើសរើសយក Disable ឬ Enable

១១. រួចអ្នកចុចពាក្យ Save Setting នោះវានឹងលោតឡើងនៅពីក្រោមនៃ Policy Tab ។



### រូបភាពទី ៣៥ ៖ បង្ហាញអំពីការរក្សាទុកនៃ Website Filter

### ៣.២ សន្តិសុខអាអ់សេសអ័ញ (Access Point Security)

ដើម្បើធ្វើអោយ Wireless Access Point របស់អ្នកមានសុវត្ថិភាពខ្ពស់ យើងសូមណែនាំវិធី សាស្ត្រទាំង ៨ ចំណុចដូចខាងក្រោម៖

១. នៅខាងក្រោមផ្នែកខាងឆ្វេងនៃពាក្យឋា Setup នៃ Window សូមចុចនៅលើពាក្យឋា Wireless Setting

Ptp-link	450M Wireless N Router Model No. TL-WR940N			
Status				
Quick Setup				
WPS	Wireless Settings			Wireless Settings Help
Working Mode				Note: The operating distance or range of your wireless connection va significantly based on the physical placement of the Router. For best resu
Network	Wireless Network Name:	Reaksa	(Also called the SSID)	place your Router.
Wireless				<ul> <li>Near the center of the area in which your wireless stations operate</li> </ul>
Wireless Settings	Mode:	11bon mixed		<ul> <li>In an elevated location such as a high shelf.</li> <li>Away from the potential sources of interference, such as fit</li> </ul>
Wireless Security	Channel Width	Auto		microwaves, and cordless phones.
Wireless MAC Filtering	Channel Width	Auto		With the Antenna in the upright position.     Away from large metal surfaces.
Wireless Advanced	Channel	Auto		Note: Failure to follow these guidelines can result in significant perform
Wireless Statistics				degradation or inability to wirelessly connect to the Router.
uest Network				Wireless Network Name - Enter a value of up to 32 characters. The Name (SSID) must be assigned to all wireless devices in your network.
HCP		Enable Wireless Router Radio		Mode - Select transmission mode according to your wireless devices.
orwarding		Enable SSID Broadcast		Channel Width - The bandwidth of the wireless channel
ecurity		Enable WDS Bridging		Channel - This field determines which operating frequency will be used
arental Control				not necessary to change the wireless channel unless you notice interfe problems with another nearby access point. If you select auto, then A
ccess Control		Save		choose the best channel automatically.
dvanced Routing				Enable Wireless Router Radio - The wireless radio of the Router co
andwidth Control				wireless stations will be able to access the Router. Otherwise, will stations will not be able to access the Router.
P & MAC Binding				Easter SSID Broadcast If you colect the Easter SSID Broad
Ivnamic DNS				checkbox, the wireless router will broadcast its name (SSID) on the air.
v6 Support				Enable WDS Bridging - You can select this to enable WDS Bridging
vstem Tools				checkbox is selected, you had better make sure the following setting
ogout				correct
2007				SSID (to be bridged) - The SSID of the AP your Router is going to cor to as a client. You can also use the survey function to select the SSID to
				BSSID (to be bridged) - The BSSID of the AP your Router is goin

### រូបភាពទី ៣៦ ៖ បង្ហាញអំពីការបើកដំណើរការ Access Point Security

២. នៅខាងក្រោមពាក្យថា Wireless Network បញ្ចូលឈ្មោះដែលត្រូវបានអោយដឹងថាជា SSID (Service Set Identifier) សម្រាប់ប្រព័ន្ធបណ្តាញរបស់ផ្ទះរបស់អ្នក៕ SSID របស់លោកអ្នកអាច មានចំនួនរហូតដល់ទៅ ៣២ តួរអក្សរ ដែលជា Case Sensitive (Example: HOME123456789 ដែលវាមានភាពខុសគ្នាពី Home123456789)

៣. ខាងក្រោម Security Options ជ្រើសរើសយកពាក្យក្នុងចំណោម Setting ដែលមានបង្ហាញ ដំណើរការបន្ទាប់គឺស្ថិតនៅក្នុងជំហ៊ានទី៤ ហើយបន្តបន្ទាប់ទៀតនៅក្នុងជំហ៊ានទី៧៕ អ្នកគួរតែ ជ្រើសរើសយកជម្រើសដែលរឹងមាំបំផុតដែលមាននៅក្នុង Wireless Access Point (WPA-PSK [TKIP] + WPA2-PSK [AES] ) ហើយប្តូរ Wireless Password៕

	450M Wireless N Router	
tp-link	Model No. TL-WR940N	
Status		
Quick Setup	WPA/WPA2 - Personal(Record)	nmended)
WPS	Version:	WPA2-PSK 🗸
Working Mode	Encryption:	AES 🗸
Network	Wireless Password:	54811430 KongReaksa@123
Wireless		(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)
- Wireless Settings	Group Key Update Period:	0 Seconds
- Wireless Security		(Keep it default if you are not sure, minimum is 30, 0 means no update)
- Wireless MAC Filtering		
- Wireless Advanced	WPA/WPA2 - Enterprise	
- Wireless Statistics	Version:	Automatic V
Guest Network	Encryption:	Automatic 🗸
DHCP	Radius Server IP:	
Forwarding	Radius Port:	1812 (1-65535, 0 stands for default port 1812)
Security	Radius Password:	
Parental Control	Group Key Update Period:	0 (in second, minimum is 30, 0 means no update)
Access Control		
Advanced Routing	Time:	
Bandwidth Control	Type.	
IP & MAC Binding	WEP Key Format:	
Dynamic DNS	Key Selected	WEP Key Key Type
IPv6 Support	Key 1: 💿	Disabled ~
System Tools	Key 2: 🔵	Disabled 🗸
Logout	Key 3: 🔵	Disabled V
	Key 4: 🔵	Disabled V

រូបភាពទី ៣៧ ៖បង្ហាញអំពីការប្តូរ នឹង Configure នៅលើ Access Point Security

៥.នៅខាងក្រោមចំណុច Security Encryption(WEP) ប្តូរ Authentication Type ទៅជា Automatic Encryption Strength ទៅជា 64bit or 128 bit. (128 bit គឺជាជម្រើសល្អ) ៕ ប្រសិនបើអ្នកមាន ឧបករណ៍ដែលមិនអាចតភ្ជាប់ទៅកាន់ប្រព័ន្ធបណ្តាញរបស់អ្នកបាន អ្នកគួរតែប្តូរ Authentication Type ទៅជា Open System ឬ Share Key ៕ ពេលខ្លះវាមានភាពចាំបាច់សម្រាប់ wireless card ឬ operating systems ៕

៥.នៅខាងក្រោម Security Encryption (WEP)Key អ្នកអាចបញ្ចូលឃ្លាសម្ងាត់ (passphrase) ហើយចុចលើប៊ូតុង Generate ដើម្បើដំណើរការដោយស្វ័យប្រវត្តិរបស់ WEP keys៕ ប្រសិនបើ អ្នកជ្រើសរើសយក Encryption Strength 64 bit four keys មានលេខប្រព័ន្ធគោល១៦ ចំនួន១០ ខ្ទង់ (0-9 A-F) ត្រូវបានបង្កើតឡើង៕ បើអ្នកជ្រើសរើសយក Encryption Strength 128 bit one key មានប្រព័ន្ធគោល១៦ ចំនួន ២៦ខ្ទង់ត្រូវបានបង្កើតឡើង៕ ម្យ៉ាងទៀត អ្នកអាចបញ្ចូលប្រព័ន្ធ គោល១៦តែមួយ សម្រាប់ WEP ៕ សាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច

Туре:	Open System 🗸	
WEP Key Format:	Hexadecimal ~	
Key Selected	WEP Key	Кеу Туре
Key 1: 🔘		128bit 🗸
Key 2: ()		128bit 🗸
Key 3: 🔿		128bit 🗸
Key 4: 🔿		128bit 🗸

Save

# រូបភាពទី ៣៨ ៖ បង្ហាញអំពីការ Configure ក្នុង WEP នៅលើ Access Point Security

WPA/WPA2 - Personal(Recommendation)	nmended)	
Version:	WPA2-PSK V	
Encryption:	AES 🗸	
Wireless Password:	KongReaksa@123	
	(You can enter ASCII characters between 8	and 63 or Hexadecimal characters between 8 and 64.)
Group Key Update Period:	0 Seconds	
	(Keep it default if you are not sure, minimun	n is 30, 0 means no update)
O WPA/WPA2 - Enterprise		
Version:	WPA2 V	
Encryption:	AES 🗸	
Radius Server IP:		
Radius Port:	1812 (1-65535, 0 stands for default	port 1812)
Radius Password:		
Group Key Update Period:	0 (in second, minimum is 3	0, 0 means no update)
Туре:	Shared Key V	
WEP Key Format:	Hexadecimal ~	
Key Selected	WEP Key	Кеу Туре
Key 1: 🔿	000000000000000000000000000000000000000	128bit 🗸
Key 2: 🔘	000000000000000000000000000000000000000	128bit 🗸
Key 3: 🔿	000000000000000000000000000000000000000	128bit 🗸
Key 4: 🔿	000000000000000000000000000000000000000	128bit 🗸

# រូបភាពទី ៣៩ ៖ បង្ហាញអំពីដំណាក់កាលចុងក្រោយ Configure នៅលើ Access Point Security

៦. ចុចពាក្យថា Apply អ្នកបានបញ្ចប់ក្នុងការដំឡើង ប្រសិនបើការដំឡើង WEP មានភាពស្មុគ ស្មាញពេកអ្នកអាចជ្រើសរើសជម្រើសសុវត្តិភាពផ្សេងទៀតដូចជា(WPA-PSK [TKIP] + WPA2-PSK [AES]) ដែលវាមានភាពងាយស្រួលក្នុងការដំឡើង នឹងសុវត្តិភាពខ្ពស់ជាង WEP៕ ៧. ប្រសិនបើអ្នកសម្រេចចិត្តជ្រើសរើសយក WPA-PSK [TKIP] ឬ WPA2-PSK [AES] ចុចលើ ជម្រើសនៅខាងក្រោម Security Options៕

៨. បញ្ចូលឃ្លាសម្ងាត់(passphrase) ចន្លោះពី ៨ ទៅ ៦៣ត្វូ ហើយបន្ទាប់ចុច Apply៕

វិធីសាស្ត្រដែលល្អបំផុតរបស់ Wireless Internet Security ប្រសិនបើអ្នកមានជម្រើស ខាង ក្រោមនេះគឺជា lists របស់ security protocols ដែលរៀបពីលំដាប់ខ្លាំង ទៅ ខ្សោយ៖

- 1. WPA3
- 2. WPA2 Enterprise
- 3. WPA2 Personal
- 4. WPA + AES
- 5. WPA + TKIP
- 6. WEP
- 7. Open Network (no security implemented

ព.៣ សត្តិសុខទីនជ្ (Endpoint Windows Security)

វីនដូគឺជាប្រព័ន្ធប្រតិបត្តិការកុំព្យូទ័រពេញនិយមមួយលើពិភពលោក។ មានបច្ចេកទេសជា ច្រើនក្នុងការធានាសន្តិសុខលើកុំព្យូទ័រក្នុងបណ្តាញ ជាពិសេស កុំព្យូទ័រដែលភ្ជាប់ទៅអ៊ីនធឺណិត។

ព.ព.១ អេទ្រខ់ឆ្លានរទស់ Windows Defender (Smart Screen)

អេក្រង់ឆ្លាតជួយការពារនិយោជិក ប្រសិនបើពួកគេព្យាយាមចូលមើលគេហទំព័រដែលបាន រាយការណ៍ពីមុនថាមានផ្ទុកនូវឧបាយឬម៉ាល់វែរ ហើយដើម្បីបញ្ឈប់ពួកគេពីការទាញយកឯក សារដែលអាចបង្កគ្រោះថ្នាក់ៗ វាក៏អាចជួយការពារប្រឆាំងនឹងការផ្សាយពាណិជ្ជកម្មក្លែងក្លាយ គេ ហទំព័របោកប្រាស់ និង រង្វាយប្រហាផ្សេងៗ។

លោក Benoit បានមានប្រសាសន៍ថា «នេះគឺជាផ្នែកមួយនៃស្រទាប់ការពារជាច្រើននៅ ក្នុងយុទ្ធសាស្ត្រប្រឆាំងឧបាយនិងម៉ាល់វែរ។ ដើម្បីប្រើប្រាស់នឹងបើកដំណើរការនៃអេក្រង់ឆ្លាតរបស់ Window Defender (Smart Screen ) យើងត្រូវធ្វើដូចលំនាំខាងក្រោម៖

១. ចុចប៊្វិតុង Start រួចស្វែងរកពាក្យថា Setting



### រូបកាពទី ៤០ ៖ បង្ហាញពីផ្ទាំង Search Engine

២. បន្ទាប់មកស្វែងរកពាក្យ Update & Security



## រូបភាពទី ៤១ ៖ បង្ហាញពីផ្ទាំង Setting

#### ៣. បន្ទាប់មកស្វែងរកពាក្យ Update & Security រួចចុចលើ App & Browser Control



### រូបភាពទី ៤២ ៖ បង្ហាញផ្ទាំងនៃ Window Security

#### ៤. បន្ទាប់មកបើកដំណើរការនៃ Window Smart Screen



#### រូបភាពទី ៥៣ ៖ បង្ហាញការបើដំណើរការនៃ SmartScreen

### 

កម្មវិធីឆ្នាំផ្តល់ការការពារប្រឆាំងនឹងកិច្ចកំហែងកម្រិតខ្ពស់ ដែលបើករង្វាយប្រហារលើ Microsoft Edge ដោយប្រើបច្ចេកវិទ្យានិម្មិតូបនីយកម្ម Hyper-V របស់ Microsoft ។ មុខងារនេះ ដំណើរការជាមួយបច្ចេកទេសបញ្លីស(Whitelist) (អ្នកប្រើអាចកំណត់វេបសាយដែលអាចទុកចិត្ត ដើម្បីអាចច្បោលវាដោយសេរីក្នុងការមើលព័ត៌មាន)។ ប្រសិនបើទំព័រវេបមិនគូរឱ្យទុកចិត្ត កម្មវិធី ឆ្នាំនឹងដាក់វាក្នុងកន្លែងមួយ ដោយប្លុកវាទាំងស្រុងពីការចូលប្រើមេម៉ូរី ទីផ្ទុក កម្មវិធី ឧបករណ៍ ផ្សេងទៀតលើបណ្តាញ ឬ ធនធានទាំងឡាយដែលជាចំណាប់អារម្មណ៍ចំពោះអ្នករង្វាយប្រហារ។ ដើម្បីប្រើប្រាស់នឹងបើកដំណើរការនៃ Window Defender យើងត្រូវធ្វើដូចលំនាំខាងក្រោម៖

១. ដំបូងយើងវាយពាក្យ Window Security នៅក្នុង Search Engine



រូបភាពទី ៤៤ ៖ បង្ហាញអំពីផ្ទាំង Search Engine

#### ២. បន្ទាប់មកយើងស្វែងរកពាក្យVirus & Threat Protection រួចលើ វាពីរដង



#### រូបភាពទី ៤៥៖ បង្ហាញអំពីផ្ទាំង Security at a glance

៣. បន្ទាប់មកយើងស្វែងរកពាក្យ Virus & Threat Protection Protection Setting រួចចុចនៅលើ Manage Setting



## រូបភាពទី ៤៦ ៖ បង្ហាញអំពីផ្ទាំង Virus & Threat Protection

### ៥. បន្ទាប់មកយើងស្វែងរកពាក្យ Real-time Protection នឹងបើកដំណើរការ



### រូបភាពទី ៤៧ ៖ បង្ហាញអំពីការបើកដំណើរការ Window Defender

៣.៣.៣ លេះគ្លួនភះ User Account Control

UAC ការពារអ្នកប្រើប្រាស់ ដោយរារាំងម៉ាល់វែរពីការបំផ្លាញកុំព្យូទ័រនិងជួយស្ថាប័នដាក់ ពង្រាយការគ្រប់គ្រង។ ពេលមុខងារនេះបើកដំណើរការ កម្មវិធីនិងភារកិច្ចតែងតែដំណើរការនៅ ក្នុងបរិបទសន្តិសុខនៃអត្តនាមធម្មតា (non-admin account)។ វាក៏អាចរារាំងដោយស្វ័យប្រវត្តិ ចំពោះការដំឡើងកម្មវិធីដែលគ្មានការអនុញ្ញាត និងការពារការផ្លាស់ប្តូរដោយចៃដន្យណាមួយ ចំពោះប្រព័ន្ធ។

ដើម្បីបើកនូវដំណើរការរបស់ User Account Control យើងត្រូវធ្វើតាមលំនាំដូចខាងក្រោម៖

60

១. ដំបូងយើងត្រូវចូលក្នុង Search រួចវាយពាក្យថា Change User Account Control Setting



## រូបភាពទី ៥៨ ៖ បង្ហាញពីការស្វែងរកនៃ UAC

២. បន្ទាប់មកយើងអាចជ្រើសរើសនូវអ្វីដែលយើងចង់បាន



## រូបភាពទី ៥៩ ៖ បង្ហាញពីការជ្រើសរើសនៃការប្រើប្រាស់ UAC

### ៣.៣.៤ ឆ្នាំឧទភរស៍ទេស Windows Defender

លោក Benoit បាននិយាយថា ឆ្នាំឧបករណ៍នេះទាក់ទងនឹងការធ្វើបញ្ឈីសលើជ្រាយវើ និងកម្ម វិធី។ វាដំណើរការលើសមាសធាតុពីរយ៉ាង៖ ទីមួយ Kernel mode code Integrity (KMCI) ដែល ការពារប្រសេសរបស់ខឺណែលនិងការពារជ្រាយវើ ពីរង្វាយប្រហារថ្ងៃដំបូង (zero-day) និង កម្សោយដទៃទៀតដោយប្រើអេជវីស៊ីអាយ (HVCI)។ ទីពីរ user mode code integrity (UMCI) គឺ ជាការធ្វើបញ្ជីសកម្មវិធីដែលប្លុកកុំព្យូទ័រ ដោយប្រើត្រឹមតែកម្មវិធីក្នុងបញ្ជី។



រូបភាពទី ៥០ ៖ បង្ហាញពី Edit Group Policy

#### ២. បន្ទាប់មកចុចលើ Computer configuration



### រូបភាពទី ៥១៖ បង្ហាញពី Local Group Policy Editor

៣. រូចចុចលើ Administrative templates.



### រូបភាពទី ៥២៖ បង្ហាញពី Administrative ក្នុង Local Group Policy Editor

#### ៤. ចុចលើ Windows components



រូបភាពទី ៥៣៖ បង្ហាញពី Window Components

៥. បន្ទាប់មកឈើងស្វែងរកពាក្យ Window Defender Application Guard



រូបភាពទី៥៤ ៖ បង្ហាញពីផ្ទាំង Window Defender Application Guard

#### ៦. បន្ទាប់មកយើងចុចលើពាក្យ Turn on Window Application Guard



រូបភាពទី ៥៥ ៖ បង្ហាញពីផ្ទាំងពីការបើកនៃ Window Application Guard

#### ៧. បន្ទាប់មកយកពាក្យឋា Enable រួច Apply បន្ទាប់មកចុចពាក្យ OK

🐏 Turn on Window	s Defender Applica	ition Guard in En	terprise Mode				
Turn on Window	vs Defender Applica	ation Guard in Er	terprise Mode	Previous Setting	Next Setting		
Not Configured	Comment:						
Enabled							
Disabled							
	Supported on:	At least Window	ws 10 Enterprise				
)ptions:			Help:				
Options: 0. Disable Windows ( Microsoft Edge ONI 2. Enable Windows ( Microsoft Office ON 3. Enable Windows ( Microsoft Edge ANC	Defender Applica Defender Applicatio V Defender Applicatio ILY Defender Applicatio Defender Applicatio O Microsoft Office	tion Guard on Guard for on Guard for	Application Gua virtualized envi virtualizetion-b improper user i compromise th virtualized envi lf you enable th organization.	ard uses Windows Hyr ronment for apps tha ased security isolatior interactions and app v e kernel or any other ronment. his setting, Applicatior	pervisor to create t are configured t n. While in isolatic ulherabilities can apps running out	a o use on, 't side of t on for ye	he

### រូបភាពទី ៥៦ ៖ បង្ហាញពីផ្ទាំងពីការបើកនៃ Window Application Guard

### ព.ព.៥ ឆ្នាំ Exploit ទេស Windows Defender

ថ្មាំ Exploit ជាប្រព័ន្ធបង្ការល្មួចរបស់វីនដូ ដែលអាចការពារប្រឆាំងនឹងរង្វាយប្រហារផ្សេងៗ និង ការពារកម្សោយនៅក្នុងវីនដូ។ វាក៏អាចការការពារកម្មវិធីចាស់ៗផងដែរ រួមមានថ្មាំកូដ ប្លុករូបភាព ប្លុកពុម្ពអក្សរមិនស្គាល់។ លោក Benoit បានប្រសាសន៍ថា លក្ខណៈនេះជួយសវនាករ កំណត់រចនា សម្ព័ន្ធនិងគ្រប់គ្រងការបន្ធូបន្ថយ Exploit ប្រព័ន្ធនិងកម្មវិធីរបស់វីនដូ ហើយវាក៏ផ្តល់ប្រភេទសមត្ថ ភាពថ្មីសម្រាប់រារាំងល្មច" ។

ដើម្បីបើកដំណើរការឆ្នាំ Explorit របស់ Window Defender យើងត្រូវធ្វើតាមលំនាំដូចខាង ក្រោម៖



១.ចុចលើ Window Search ស្វែងរកពាក្យ " Edit Group Policy"

រូបភាពទី ៥៧ ៖ បង្ហាញពី Edit Group Policy

#### ២. បន្ទាប់មកចុចលើ Computer configuration



#### រូបភាពទី ៥៨៖ បង្ហាញពី Local Group Policy Editor

៣. រួចចុចលើ Administrative templates.



### រូបភាពទី ៥៩៖ បង្ហាញពី Administrative ក្នុង Local Group Policy Editor

#### ៤. ចុចលើ Windows components

🧾 Local Group Policy Edito	r		-	Х
File Action View Help	)			
🗢 🔶 🙍 🖬 📓	1			
Local Computer Policy	C Administrative Templates			
<ul> <li>Computer Configurat</li> <li>Software Settings</li> </ul>	Windows Components	Setting		
Windows Setting:     Windows Setting:     Administrative Te	Description: Contains settings for operating	Network		
Control Panel     Control Panel     Detwork     Printers	system components.	Server		
Server		System		
System     System     System		All Settings		
<ul> <li>All Settings</li> <li>User Configuration</li> </ul>				
Software Settings     Get Windows Settings     Administrative Te				
Administrative le				
		¢		 >
, , ,				

### រូបភាពទី ៦០៖ បង្ហាញពី Window Components

៥. បន្ទាប់មកចុចលើ Windows Defender Exploit Guard



រូបភាពទី ៦១៖ បង្ហាញពី Window Defender Exploit Guard

#### ៦.បន្ទាប់មកចុចលើExploit Protection

I Local Group Policy Edito	pr		-	Х
File Action View Help	)			
🗢 🏟 🙎 🖬 🗟				
Presen ^ Push Ta	Windows Defender Exploit Guar Exploit Protection	d Setting		
RSS Fe		Exploit Protection		
Securit Shutdo				
Softwa				
Speech Store				
> 🛄 Tablet Task Sc				
Text Inj Windo				
Windo				
→ Windo Windo Windo		<		>
<pre></pre>	Extended Standard			

### រូបភាពទី ៦២៖ បង្ហាញពី Exploit

៧.បន្ទាប់មក ចុចលើ Use a common set of exploit protection settings.



រូបភាពទី ៦៣ ៖ បង្ហាញពី Use a common set of exploit protection

## ៨.ចុចលើ Enabled and រួចចុចពាក្យ OK.

Use a common set of the observation of the observat	exploit protect	tion settings	Previous Setting Next Setting
<ul> <li>Not Configured</li> <li>Co</li> <li>Enabled</li> </ul>	omment:		
			^
O Disabled Su	ipported on:	At least Windo	ws Server 2016, Windows 10 Version 1709
Options:			Help:
Type the location (local pa the mitigation settings co	ath, UNC path, onfiguration XI	or URL) of ML file:	Specify a common set of Windows Defender Exploit Guard system and application mitigation settings that can be applied to all endpoints that have this GP setting configured. There are some prerequisites before you can enable this setting: - Manually configure a device's system and application mitigation settings using the Set-ProcessMitigation PowerShell cmdlet, the ConvertTo-ProcessMitigationPolicy PowerShell cmdlet, or directly in Windows Security Generate an XML file with the settings from the device by running the Get-ProcessMitigation PowerShell cmdlet or using the Export button at the bottom of the Exploit Protection area in Windows Security Place the generated XML file in a shared or local path. Note: Endpoints that have this GP settings set to Enabled must be able to access the XML file, otherwise the settings will not be applied. Enabled

#### រូបភាពទី ៦៤៖ បង្ហាញពី Enable Window Defender Exploit Guard

#### n.n.b Microsoft Bitlocker

លោក Benoit បានមានប្រសាសន៍ថា "Bitlocker គឺជាដំណោះស្រាយក្ខដនីយកម្មទូទាំង ជ្រាយក្នុងវីនដូ ១០ Professional និង Enteprise។ វាជួយកាត់បន្ថយអាក់សសទិន្នន័យដែលគ្មាន ការអនុញ្ញាត ដោយពង្រឹងការការពារប្រព័ន្ធនិងឯកសារ និងបញ្ហូនទិន្នន័យដែលមិនអាចអាក់ សេសបាន ប្រសិនបើកុំព្យូទ័រត្រូវបានបំបែកឬកែច្នៃឡើងវិញ។

លោកបានបន្ថែមថា "នេះពិតជាសំខាន់ណាស់ - អ្នកមិនចង់ក្លាយជាមនុស្សដែលត្រូវបានស្ដី បន្ទោស បន្ទាប់ពីបាត់បង់ឧបករណ៍ ទិន្នន័យ លេចធ្លាយព័ត៌មានរបស់ស្ថាប័ន្ន " ។

ដើម្បីបើកដំណើរការនៃ Microsoft Bitlocker យើងត្រូវធ្វើតាមលំនាំដូចខាងក្រោម៖

១. ចុចលើ Window Search ហើយស្វែងវកពាក្យ Manage BitLocker

=	All Apps Documents Web More 🔻	R
ŵ	Best match	
0	Manage BitLocker Control panel	
Þ	Apps	Manage BitLocker
	SQL Server 2014 Management > Studio	Control panel
	Manage Help Settings >	C Open
	Internet Download Manager	
	Internet Information Services (IIS)     Manager	
	Settings	
	RE Manage your account >	
	☑ Manage work or school account >	
	IE Manage app execution aliases >	
٨,	G Manage what Cortana can do, see, → and use	
ŝ	Image map updates     >	
2	Search the web	
	$\rho$ manage	i 🕂 💽 🧮 🖶 💼 💌 😪 💷

រូបភាពទី ៦៥៖ បង្ហាញពី Manage BitLocker

២. Turn on BitLocker



### រូបភាពទី ៦៦ ៖ បង្ហាញពី Turn On BitLocker

1

ព.ព.៧ ឆ្លាំ Credential ទេស់ Windows Defender

ឆ្នាំ Credential ជាបច្ចេកទេសសន្តិសុខនិម្មិតក្នុងការដាក់ទិន្នន័យសម្ងាត់ឱ្យនៅដាច់ដោយឡែក ដើម្បីឱ្យត្រឹមតែប្រព័ន្ធប្រតិបត្តិការប៉ុណ្ណោះអាចធ្វើការអាក់សេសវា ដោយការពារពីរង្វាយប្រហារ លួចអត្តនាម (user account)។ លក្ខណៈនេះផ្តល់នូវសន្តិសុខហាដវៃរនិងការការពារប្រសើរជាងមុន ប្រឆាំងនឹងកិច្ចកំហែងឥតឈប់ឈរ។

ដើម្បីបើកដំណើរការឆ្នាំ Credential របស់ Window Defender យើងត្រូវធ្វើតាមលំនាំដូចខាង ក្រោម៖



១. ចុចលើ Window Search រួចវាយ ពាក្យ Edit Policy Group

### រូបភាពទី ៦៧ ៖ បង្ហាញពី Edit Group Policy

២. បន្ទាប់មកចុចយកពាក្យ Computer Configuration



## រូបភាពទី ៦៨៖ បង្ហាញពី Local Group Policy Editor

៣. បន្ទាប់មកចុច លើ Administrative Templates



## រូបភាពទី ៦៩៖ បង្ហាញពី Administrative ក្នុង Local Group Policy Editor

#### ៤. រួចចុចលើពាក្យ System

Local Group Policy Editor	r		-	×
File Action View Help				
🗢 🔿 🖄 🖬 🔒				ţ
Computer Policy mputer Configuration Software Settings Windows Settings Administrative Templates Control Panel	Administrative Templates System Description: Allows configuration of various system component settings.	Setting Control Panel Network Printers Server		- -   ;
<ul> <li>Printers</li> <li>Server</li> <li>Start Menu and Taskbar</li> <li>System</li> <li>Windows Components</li> <li>All Settings</li> <li>c Configuration</li> </ul>		<ul> <li>Start Menu and Taskbar</li> <li>System</li> <li>Windows Components</li> <li>All Settings</li> </ul>		1 
Software Settings Windows Settings Administrative Templates				:      
< >	Extended Standard	¢		>

### រូបភាពទី ៧០៖ បង្ហាញពី System នៅក្នុង Local

### ៥. បន្ទាប់មកចុច Device Guard



#### រូបភាពទី ៧១៖ បង្ហាញពី Device Guard នៅក្នុង Local Group Policy

និស្សិត៖ គង់ រក្សា និង សន សំខាន់

ឌ៤

សាស្ត្រាចារ្យណែនាំ៖ បណ្ឌិត លឹម សេងឌ័

#### ៦. ចុចលើពាក្យ Turn on Virtualization Based Security



#### រូបភាពទី ៧២៖ បង្ហាញពី Turn on Virtualization Based Security

#### ៧. បន្ទាប់មកចុច Enable រួចចុច OK

l l I Turn On Virtualiza	ックレン しょうしん Pased Securi	ty							$\times$
Turn On Virtualiza	ation Based Securi	ty		Previous Se	etting				
<ul> <li>Not Configured</li> <li>Enabled</li> </ul>	Comment:								^
O Disabled	Supported on:	At least Window	vs Server 2016	, Windows 10	)				~ ~
Options:			Help:						
Select Platform Secur	ity Level:		Specifies w	nether Virtual	ization Based	d Security is en	abled.		<b>`</b>
Secure Boot and DM/ Virtualization Based P Not Configured	A Protection Protection of Code	v Integrity:	Virtualizatio provide sup requires Sec of DMA Pro and will onl	on Based Secu oport for secu cure Boot, and tections. DM/ y be enabled	urity uses the irity services. d can option A protections on correctly	Windows Hyp Virtualization I ally be enabled s require hardw configured de	ervisor Based So I with th are sup vices.	to ecurity he use oport	
Credential Guard Con	figuration:		Virtualizatio	on Based Prot	ection of Co	de Integrity			
Not Configured	~		This setting Mode Code	enables virtu Integrity. Wi	ualization bas hen this is en	sed protection abled, kernel n	of Kern node m	el emory	
Secure Launch Config	guration:		protections protected b	are enforced y the Virtuali	and the Cod zation Based	le Integrity vali Security featu	dation re.	path is	
Not Configured	~		The "Disabl Code Integr "Enabled wi	ed" option tu rity remotely thout lock" o	rns off Virtua if it was previ ption.	alization Based iously turned c	Protect on with	tion of the	
			The "Enable	d with UEFI l	ock" option e	ensures that Vir	tualizat	tion	~
					ОК	Cancel		Apply	

#### រូបភាពទី ៧៣៖ បង្ហាញពី Enable Window Defender Credential Guard

និស្សិត៖ គង់ រក្សា និង សន សំខាន់

សាស្ត្រាចារ្យណែនាំ៖ បណ្ឌិត លឹម សេងឌី

# ព.៤ តេស្តសត្តិសុខ (Security Testing)

## ពា.៤.១ មេរៀមតំន្មើទនៃសូខ្សែ Nmap

ដើម្បីតំឡើងកម្មវិធី យើងគូរតែធ្វើតាមលំនាំនៃការតំឡើងដូចខាងក្រោម៖

១.ចុចបើកដំណើរការ nmap file ដែលអ្នកបាន download ហើយបន្ទាប់មកចុចពាក្យថា I Agree-

>Next->Install->Next->Finish ដែលមានបង្ហាញតាមលំដាប់លំដោយដូចរូបខាងក្រាមនេះ៖



រូបភាពទី ៧៤៖ បង្ហាញពីការ Install Nmanp នៅលើ Window



## រូបភាពទី ៧៥៖ បង្ហាញពីការ Install Nmanp នៅលើ Window

🗑 Nmap Setup		_		×
Choose Install Location				NUMBER
Choose the folder in which to install Nmap.				J
Setup will install Nmap in the following folder. To install in a select another folder. Click Install to start the installation.	differen	t folder, clid	k Browse	and
Destination Folder				
C:\Program Files (x86)\Nmap		Bro	wse	
Space required: 83.4MB				
Space available: 164.3GB				
Nullsoft Install System v2.51				
< Bad	c 🗌	Install	Ca	ncel

## រូបភាពទី ៧៦៖ បង្ហាញពីការ Install Nmanp នៅលើ Window

🌍 Nmap Setup		_	
Installation Complete Setup was completed successfully.			
Completed			
Show details			
Nullsoft Install System v2.51			
	< Back	Next >	Cancel

រូបភាពទី ៧៧៖ បង្ហាញពីការ Install Nmanp នៅលើ Window



## រូបភាពទី ៧៨៖ បង្ហាញពីការ Install Nmanp នៅលើ Window



### រូបភាពទី ៧៩៖ បង្ហាញពីការ Install Nmanp នៅលើ Window

## **៣.៤.២. មេរៀមតំនេ្ប៏ទស្**ស្វ៊ែ Nessus

ដើម្បីធ្វើការសាកល្បងណែតវ៉ឹករបស់យើងថាតើមាន សុវត្ថិភាពឬមួយមិនមាន យើងអាចប្រើ ប្រាស់នូវ ស្ងហ្វ៊ៃ Nessus ។ ដូចនេះដើម្បីប្រើប្រាស់នូវ ស្ងហ្វ៊ែនេះបានយើងគូរដំឡើងវា តាម ដំណាក់ដូចខាងក្រោម៖

#### ១. ដំបូងយើងត្រូវចូលទៅក្នុង Web Browser រួចវាយពាក្យ Download Nessus

www.tenable.com > downloads > nessus \* Download Nessus | Tenable® Download Nessus and Nessus Manager. ... In order to complete your Nessus installation, you need an activation code if you don't have one already.

www.tenable.com > products > nessus Download Nessus Vulnerability Assessment | Tenable® Download Nessus vulnerability assessment solution, trusted by more than 27000 organizations worldwide as one of the most widely deployed security ... Nessus Essentials - Nessus Professional - See how we compare. You've visited this page 2 times. Last visit: 9/24/20

### រូបភាពទី ៨០៖ បង្ហាញអំពិការដោតឡូត ស្វហ្វ៊ៃ Nessus

#### ២. បន្ទាប់ពីយើងទទួលបានហើយ យើងចុចពីរដឹងទៅ Software Nessus

💐 Edraw.Max.9.4.0.688.Portable.rar	3/3/2020 8:26 AM	WinZip File	249,534 KB
🚯 metasploit-latest-windows-x64-installer	8/29/2020 3:01 PM	Application	214,689 KB
🖟 Nessus-8.11.1-x64.msi	8/29/2020 7:26 PM	Windows Installer	74,299 KB
🕝 nmap-7.80-setup.exe	8/29/2020 2:17 PM	Application	26,292 KB

#### រូបភាពទី ៨១ ៖ បង្ហាញអំពី File Of Nessus

#### ៣. បន្ទាប់មកយើងចុចពាក្យថា Next



## រូបភាពទី ៨២៖ បង្ហាញអំពីការដោតឡូត សូហ៊្វែ Nessus

## ៥. បន្ទាប់មកឈើងចុចពាក្យថា I Accept the Term in the License Agreement

License Agreement	WIZU G		44
Please read the following license agreer	ment carefully.		
			^
*** <u>I</u>	MPORTANT***		
THIS AGREEMENT IS INTEN	DED TO BE LEG	ALLY BIND	ING. BY
ICLICKING THE "AGREE" OR			
CONTINUING TO DOWNLOAD,	INSTALL OR USE	TENABLE S	OFTWARE
CONTINUING TO DOWNLOAD, AND OR SERVICES (OR AUTHO	INSTALL OR USE	TENABLE S G A THIRD	OFTWARE PARTY TO
CONTINUING TO DOWNLOAD, AND OR SERVICES (OR AUTHO DO SO ON YOUR BEHALF), YOU (1) YOUR ACCEPTANCE	INSTALL OR USE ORIZING/ALLOWING INDICATE: OF THIS AGREEME	ON BELOV TENABLE S G A THIRD	OFTWARE PARTY TO
CONTINUING TO DOWNLOAD, AND OR SERVICES (OR AUTHO DO SO ON YOUR BEHALF), YOU (1) YOUR ACCEPTANCE (2) YOU ACKNOWLEDG TERMS AND CONDITIO	INSTALL OR USE ORIZING/ALLOWING INDICATE: OF THIS AGREEME GE THAT YOU HAV NS OF THIS AGREE	ON BELOV TENABLE S G A THIRD ENT; E READ AL EMENT. UNI	COFTWARE PARTY TO L OF THE DERSTAND
CONTINUING TO DOWNLOAD, AND OR SERVICES (OR AUTHO DO SO ON YOUR BEHALF), YOU (1) YOUR ACCEPTANCE (2) YOU ACKNOWLEDG TERMS AND CONDITIO I accept the terms in the license agreem	INSTALL OR USE INSTALL OR USE ORIZING/ALLOWING INDICATE: OF THIS AGREEMI GE THAT YOU HAV NS OF THIS AGREI Inent	ON BELOW TENABLE S G A THIRD ENT; E READ AL EMENT. UNI	COFTWARE PARTY TO L OF THE DERSTAND
CONTINUING TO DOWNLOAD, AND OR SERVICES (OR AUTHO DO SO ON YOUR BEHALF), YOU (1) YOUR ACCEPTANCE (2) YOU ACKNOWLEDG TERMS AND CONDITION I accept the terms in the license agreem I do not accept the terms in the license a	INSTALL OR USE ORIZING/ALLOWINN INDICATE: OF THIS AGREEME EE THAT YOU HAV NS OF THIS AGREE Nent agreement	ON BELOW TENABLE S G A THIRD ENT; E READ AL EMENT. UNI	OFTWARE PARTY TO L OF THE DERSTAND
CONTINUING TO DOWNLOAD, AND OR SERVICES (OR AUTHO DO SO ON YOUR BEHALF), YOU (1) YOUR ACCEPTANCE (2) YOU ACKNOWLEDG TERMS AND CONDITION I accept the terms in the license agreem I do not accept the terms in the license a nstallShield	INSTALL OR USE INSTALL OR USE ORIZING/ALLOWIN INDICATE: OF THIS AGREEMI GE THAT YOU HAV NS OF THIS AGREI Hent agreement	ON BELOW TENABLE S G A THIRD : INT; E READ AL IMENT. UNI	OFTWARE PARTY TO L OF THE DERSTAND Y

## រូបភាពទី ៨៣ ៖ បង្ហាញអំពីការព្រមនៃការដោតឡូត សូហ្វ៊ែ Nessus

## ៥. បន្ទាប់មកយើងចុចពាក្យថា Next

📷 Ienable	Nessus (x64) - InstallShield V	Vizard		X
Destination	on Folder dt to install to this folder, or click	Change to install to	a different folder.	と
	Install Tenable Nessus (x64) to C:\Program Files\Tenable\Ness	:: sus\		Change
InstallShield -				
		< Back	Next >	Cancel

## រូបភាពទី ៨៤ ៖ បង្ហាញអំពីការព្រមនៃការដោតឡូត សូហ្វ៊ែ Nessus

### ៦. បន្ទាប់មកយើងចុចពាក្យថា Install



## រូបភាពទី ៨៥ ៖ បង្ហាញអំពីការព្រមនៃការដោតឡូត ស្ងហ្វ៊ែ Nessus

#### ៧. បន្ទាប់មកយើងចុចពាក្យថា Finish



### រូបភាពទី៨៦ ៖ បង្ហាញអំពីការព្រមនៃការដោតឡុត ស្វហ្វ៊ៃ Nessus
៨. បន្ទាប់មកវានឹងលោតផ្ទាំង Nessus នៅលើ Web Browser រួចចុច Connected Via SSL



រូបភាពទី ៨៧ ៖ បង្ហាញអំពីផ្ទាំង ស្ងូហ៊្វែ Nessus នៅក្នុង Web Browser

៩. បន្ទាប់មកយើងចុចលើ Processed in Localhost

Your connection is not private	
Attackers might be trying to steal your information from <b>localhost</b> (for example, passwords, messages, or credit cards). <u>Learn more</u>	
NET::ERR_CERT_AUTHORITY_INVALID	
Help improve security on the web for everyone by sending URLs of some pages you visit, limited system information, and some page content to Google. <u>Privacy policy</u> .	
Hide advanced Back to safety	
This server could not prove that it is <b>localhost</b> ; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.	
Proceed to localhost (unsafe)	

រូបភាពទី ៨៨ ៖ បង្ហាញអំពីផ្ទាំង Processed to LocalHost

### ១០. បន្ទាប់មកជ្រើសរើពាក្យ Nessus Essentials រួចចុចពាក្យ Next



រូបភាពទី ៨៩ ៖ បង្ហាញអំពីការជ្រើសរើស Nessus Essential

១១. បន្ទាប់មកយើង Register Code រួចចុចពាក្យថា Next



រូបភាពទី ៩០ ៖ បង្ហាញអំពីការវាយ Register Nessus

### ១២. រូចយើងវាយ Username នឹង Password



## រូបភាពទី ៩១ ៖ បង្ហាញអំពីការវាយ Username & Password

១៣. បន្ទាប់មកវានឹងលោតផ្ទាំងនៅក្នុង Nessus

Professional	Scans Settings	🔔 hemant 오
FOLDERS My Scans 1	My Basic Network Scan	Your trial will expire in 6 days, on Feb 16, 2020. To unlock more features and continue using Nessus Pro beyond your Trial
All Scans Trash	Hosts 0 Vulnerabilities 0 History 1	Purchase Now
	No hosts are available.	
Policies		Scan Details
Plugin Rules     Customized Reports     Scanners		Policy: Basic Network Scan Status: Running O Scanner: Local Scanner Statt. Today 2731 MA
🚇 Community		
Research		

រូបភាពទី៩២ ៖ បង្ហាញអំពីផ្ទាំងនៃការស្វែងរក Nessus Scan

# សេចភ្តីសត្ថិដ្ឋាន តិច ភាវេ្តល់អតុសាសត៍

## ១. សេខភ្តីសត្ថិដ្ឋាន

ក្រោយពីបានសិក្សាអំពីមុខវិជ្ជាសេដ្ឋកិច្ចព័ត៌មានវិទ្យាកន្នងមក យើងបានដឹងថាវាពិតជាមាន សារៈប្រយោជន៍ណាស់ចំពោះមនុស្សទូទៅ។ សម័យបច្ចុប្បន្នវិទ្យាសាស្ត្រគឺកាន់តែមានការរីក ចម្រើនឥតឈប់ឈរ ជាពិសេស ជាពិសេសគឺ វិស័យបច្ចេកវិទ្យាព័ត៌មាន ដែលត្រូវបានគេបានកំពុង អិភិវឌ្ឍន៍នានា យើងសង្កេតឃើញថាវិស័យបច្ចេកវិទ្យាព័ត៌មានកុំព្យូទ័រ កំពុងត្រូវបានយកចិត្ត ទុកដាក់យ៉ាងខ្លាំង ព្រោះវាជាកត្តាចំបងក្នុងការអភិវឌ្ឍប្រទេសជាតិ ឲ្យមានការរីកចម្រើនឡើងទៅ តាមការផ្លាស់នៃសម័យទំនើប ។ ដើម្បីធ្វើឲ្យប្រព័ន្ធណែតរ៉ឹក មានដំណើរការបានល្អ និងសុវត្ថិភាព ហើយងាយស្រួលក្នុងការគ្រប់គ្រង់ ត្រូវប្រើប្រាស់នូវឧបករណ៍ទាន់សម័យទៅតាមសង្គមយើង បច្ចុប្បន្ន កុំព្យូទ័រ ជាពិសេស ផ្នែករឹងនៃកុំព្យូទ័រ ឲ្យមានល្បើនខ្ពស់ និងការជ្រើសរើសទីតាំងនៃបរិស្ថា នជុំវិញឲ្យមានសុវត្ថិភាពខ្ពស់ ថែមទាំងអាចធ្វើការទំនាក់ទំនងគ្នាបានថែមទៀតផងដែលលក្ខណៈ បែបនេះ គេហៅថា ប្រព័ន្ធណែតរ៉ឹក ៖

- សម្រូលដល់កិច្ចការផ្សេងៗ ក្នុងដំណើរការទំនាក់ទំនងគ្នាប្រចាំថ្ងៃ ។
- មានភាពងាយស្រួលទាំងការបព្អូន នឹងទទួលព័ត៌មាន ។
- មានភាពងាយស្រួលក្នុងការគ្រប់គ្រង់ឯកសារ នឹងចែកចាយឯកសារ។

ដូច្នេះហើយ បណ្តាញប្រព័ន្ធណែតវ៉ឹក ផ្តល់នូវអត្ថប្រយោជន៍យ៉ាងច្រើនដល់មនុស្សទូទៅ គឺវា ជួយសម្រូលនូវរាល់កិច្ចការផ្សេងៗ និងការទំនាក់ទំនងយ៉ាងរហ័សទាន់ពេលវេលា ព្រមទាំងផ្តល់នូវ សុវត្ថិភាពផងដែរ ។

## ២. ನಾಣ್ಣಬೆಳುಣಾಕಾಣ್

ដើម្បីអោយប្រព័ន្ធណែតវ៉ឹកមានដំណើរល្អ និងផ្តល់ភាពងាយស្រូលដល់អ្នកប្រើប្រាស់ យើងគូរ តែមានការបន្ថែមនូវវិធីសាស្ត្រ ដើម្បីធ្វើការរៀបចំ និងធ្វើការពារចំពោះកុំព្យូទ័រនៅក្នុងប្រព្ធន័ ណែតវ៉ឹកដូចជា៖

- ធ្វើការ update នៃ software នៃកម្មវិធីប្រើប្រាស់ប្រចាំថ្ងៃ ។
- បើកដំណើរការរបស់ Firewall របស់កុំព្យូទ័រ ។

## ວິສຸຄຸລາຍຄວອ

#### ຉຘຎຎຎຎ

9. សៀវភៅ របាយការណ៍កម្មសិក្សា ការការពារប្រព្ធន័ណែតវ៉ឹក ចងក្រងដោយនិស្សត សៀង ពិ សិទ្ធ និង ជូរ ឈុនហ៊ីម នៃសាកលចិទ្យាល័យ ភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ខកិច្ច ។

U. https://searchnetworking.techtarget.com/definition/WAN-wide-area-network

m.<u>https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-</u> osi/

d. https://www.guru99.com/tcp-ip-model.html

t. https://privacy.net/how-to-secure-your-computer/

b. https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

៧. https://www.barracuda.com/glossary/network-firewall

d.https://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-

<u>and-gray-hats/</u>

e.https://www.itsupportguides.com/knowledge-base/windows-10/windows-defender-

smartscreen-prevented-an-unrecognized-app-error/

90.https://techcommunity.microsoft.com/t5/windows-insider-program/windows-defender-

application-guard-standalone-mode/m-p/66903

99.<u>https://www.howtogeek.com/howto/windows-vista/disable-user-account-control-uac-the-easy-way-on-windows-vista/</u>

១២.https://www.microsoft.com/security/blog/2017/10/23/windows-defender-exploit-guardreduce-the-attack-surface-against-next-generation-malware/

9m.https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-

guard/credential-guard

9 G.https://docs.microsoft.com/en-us/windows/security/identity-protection/credentialguard/credential-guard-manage

១ ៥.<u>https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-</u> guard/credential-guard-manage

9b. https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption

9 Ŋ.//https://itcambonews.wordpress.com/2016/05/10/%E1%9E%94%E1%9F%92%E1%9E%9 A%E1%9E%96%E1%9F%90%E1%9E%93%E1%9F%92%E1%9E%92%E1%9E%80%E1%9E %BB%E1%9F%86%E1%9E%96%E1%9F%92%E1%9E%99%E1%9E%BC%E1%9E%91%E1% 9F%90%E1%9E%9A-%E1%9E%8E%E1%9F%82%E1%9E%8F%E1%9E%9C/