

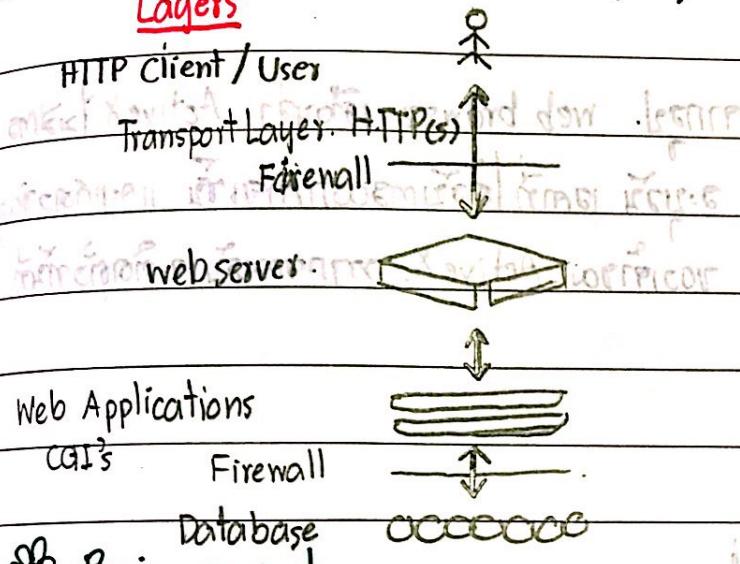
Chapter 8.

Web Security Issues and Malware

 www Security

Internet के लिए Client / Server एवं HTTP protocol

Layers



Basic concepts

browsers ანუ HTTP request უდინებს Web Server-ისგან Web server ანუ

HTTP response ດາວໂຫຼດນີ້ browser

Types of web pages

► Static ជីវិត និង សារិក អាជ្ញាក់ នូវ រួម ឱ្យ ឈរ Static ដើម្បី ការ ការ កំ សុំ ឬ កំ សុំ នៅក្នុង ការ ការ កំ សុំ

ការរំលែករបស់ទាំងអ្នកនៃវត្ថុ គាមុទ្ទី និង ការរំលែករបស់ទាំងអ្នក។

► **Dynamic** ກໍາໄວ້ເນັ້ນໄວ້ງວຍງານ **Dynamic** ຈຶ່ງມີການກົດທຳມື່າໃຫຍ່ກົມອອກໃຈຕະລາງໄວ້ການ

ສິ້ນກົງ parameter ຈົດຕະຕິໃຫຍ່ request ເຊື່ອຈາກການປະເວັດລາຍກ ໂດຍອຳນົມງານຂອງ

ឧប្បជ្ជ google map នៃការណា script តើអាកាសដីទិន្នន័យ ឬស្ថាប័នទិន្នន័យ ឬការណាទិន្នន័យ

గ්‍රෑසින් තේරුවකාග || සිංහාගයු || ගැඹු ආගත් || තෘප්ති මීම ග්‍රෑසි ගැඹු map තීමහා || ස්ථාන ගැඹු

ໄລຍະ: ມີກົດ request ໄປສ່ວນ server ແລ້ວຕັ້ງການທີ່ຈຸດ ໄລຍະ: ໂອງການຮັດໃຈໃໝ່ client ທີ່ມາ

ex. ActiveX, CGI.

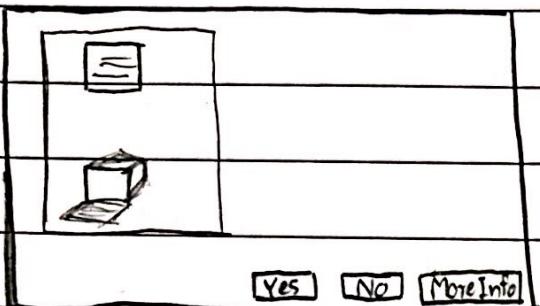
Dynamic និងការងារ

~~Subject~~ : Dynamic !!

Date :

- ① **ActiveX** មីន់ framework សំខាន់ក្នុងការកែលការណ៍ការងារ និងក្រោងកែវគ្មាន តិចតាត់ក្នុងក្រុងការ
រៀបចំ 

ActiveX មិនត្រូវការកែតម្រូវ ទាំងអស់ គ្មានការងារណាទីរបស់រួម



જાગેરું. web browser ચોંચવાં ActiveX નું ક્રમાંગ
એનુંચિં એસ્ટેપી તોંબાં કરીએ હોય || અને એનુંચિં એસ્ટેપી
જોંગ્ચાં રાખીએ ActiveX. નજીબદિને એનું એસ્ટેપી જોંગ્ચાં

Java applets vs. Javascript

► Java applets

— ପାଇଁରେ ମାତ୍ରମେ କିମ୍ବା କିମ୍ବା

ការអនុវត្តកំរិតរយៈផែកយករួចរាល់ដោយ Container

▶ Java Script

– ឧបនគរក្សាបន្ទាន់នៃ browser. និងក្រឹងការងារ.

ກົງຜລິສ ຂອບກຸມດາຂວາ.

© CGI

តើវិញ នាមទីក្រុងការរំភោគ នឹងធ្វើជា server ក្នុងមិនការណែនាំ ក្នុងការរំភោគ នឹងធ្វើជា server ក្នុងមិនការណែនាំ

PHP

Code PHP នៃមករណដោយ server ត្រូវដាក់ក្នុងការបង្កើត HTML ដើម្បីក្នុងការ

ໄປສັງ browser . ຖົກ້າ PHP ກວມກອດ ເຖິງ ດາວ ຕັ້ງ ຖື່ນ ແກ້ໄຂຕູ້າຊີ່ຕູ້າ ແລ້ວ ດີວີ່ຈະຮ່ວມຍຸດຕະກູມ server ທີ່.

សំណើរបស់ខ្លួន ដូចជា: ការអនុវត្តន៍ការងារ ការការពារ និងការសេវាភាសា

o. AJAX

use google map, gmail, youtube, facebook.

✿ Cookies for Authentication.

- តើសេវាឌែលក្នុងការកំណត់ព័ត៌មានអ្នកប្រើប្រាស់ | កិច្ចរបាយខាងក្រោម
- តើគឺត្រូវពាក្យិសនី password, username, id
- cookies នឹងត្រូវរាយការនៅ Hard disk.

Problem: ពាក្យិសនីនៅ Hard disk នឹងរាយការឡើងទៅ, និងធ្លាប់ដាក់ឡើង

✿ Single sign-on

- log-in ត្រូវធែនៅ ឬតាមពាក្យិសនីទិន្នន័យឡើង
- ex. log-in google សារអភិវឌ្ឍន៍ google drive, google sheet
"credentials" នៅក្នុងការកំណត់ព័ត៌មានអ្នកប្រើប្រាស់ user ឱ្យដោះស្រាយបាន

✿ SQL Injection.

នៅក្នុងការរួមចិត្ត DB ទិន្នន័យនៃការកំណត់ព័ត៌មាន នៅក្នុងការកំណត់ព័ត៌មាន SQL នឹងរួមចិត្តការកំណត់ព័ត៌មាន។

✿ Session Hijacking.

- សេវាឌែលក្នុងការកំណត់ព័ត៌មាន នឹងរាយការនៅក្នុង session រាយការឡើង
- សេវាឌែលក្នុងការកំណត់ព័ត៌មាន នឹងរាយការនៅក្នុងការកំណត់ព័ត៌មាន និងការកំណត់ព័ត៌មាន
- **"Droidsheep"** កំណត់ព័ត៌មាន id នៃគឺសារនៅលើ network នៅលើរាយការ

✿ Trusting the Web

1. គោរពក្រារណ៍ទាំងអស់
2. រៀបចំផែនការទៅការសំណងជាប់អ្នកក្នុងព័ត៌មាន
3. ចិត្តអ្នកដែលរាយការនៅលើការប្រើប្រាស់

Buffer Overflow.

ex. ถ้า web server เป็นตัวที่รับข้อมูล เนื่องจากตัวที่รับข้อมูล ต้องมีพื้นที่ buffer ขนาด 100 byte นั่นคือความจุ buffer ที่ว่าง空ตรงนั้น หากเราส่งมาตัวที่ต้องการจะเข้าไปใน buffer มากกว่า 100 byte นั่นคือความจุ buffer ที่ว่าง空ตรงนั้น เรียกว่า "Buffer Overflow"

Preventing stack overflow ได้ยัง...

- Hardware or OS.
- check.

Malware.

ตัวโปรแกรมที่มีไว้ทำภัยคุกคาม เช่น ไวรัส โทรทัศน์ หลักการทำงานคือ ใช้การโจมตีทางระบบ host

► Virus

เป็น program ที่ไม่ต้องการ program อื่นๆ ของตัวเองมายังเครื่องที่ใช้เครื่องของ host นะครับ ก็จะติดตามและไปกิน host รบกวนการทำงานของ host

► Worm

ตัวมันเองก็เป็น program ของการโจมตี attack result ทำให้เกิดภัยคุกคาม

► Malicious codes

- Trojan Horse.
- ตัวมันเองก็เป็น program ที่ไม่ต้องการ program อื่นๆ ของตัวเองมายังเครื่องของ host แต่ต้องการเข้าไปในเครื่องของ host แล้วก็จะติดต่อไปกับ host ต่อไป
- ตัวมันเองก็จะติดต่อไปกับ host แล้วก็จะติดต่อไปกับ host ต่อไป
- ตัวมันเองก็จะติดต่อไปกับ host แล้วก็จะติดต่อไปกับ host ต่อไป
- ตัวมันเองก็จะติดต่อไปกับ host แล้วก็จะติดต่อไปกับ host ต่อไป

• Trapdoor

เช่น ~~เช่น~~ ต้องการเข้า code ก็ต้องมีช่องทางเข้ามาช่องหนึ่ง คือหากต้องเข้าช่องนี้ ต้อง
 . ต้อง input code ที่ต้องการเข้า code นั้นๆ

► Bot

ຕາມ: ກຳ program ກ່ຽວຂ້ອງຕົກ ຕາມ: ກຳ program ກ່ຽວຂ້ອງ trojan.

► Ransomware.

ເປົ້າ program ກ່ຽວຂ້ອງຕົກ ດັ່ງນີ້ກ່ຽວຂ້ອງທີ່ຈຳຕົວ

Ransomware ສະແດງ.

1. Lock screen.

2. Encryption.: encrypt ໄຟກໍາກົມໂຄສະນິກໍາ password ເພື່ອໄຫຼືກຳນົດເກົ່າໄຕ

ສົມບັດ: disable firewall ລົດຖານ.

► Rootkit

software ກ່ຽວຂ້ອງໂອນໄດ້ຢືນ program.

► Spyware.

preventing spyware:

ຝາກໂທກຣມ ລາຍເຊັນໄວ້ຊັ້ນ

ຂອກວ່າມີມານີ້ anti spyware.

► Keylogger.

ຕັດຈຸບັນໄວ້ຊັ້ນ / ກົງການໜີ້

ສ້າງໝູນຄ່າຄຸນຊັ້ນໂລງງານ.

► Blended threat

ໄຟກໍາກົມແບກໄດ້ເກົ່າໃຈ Trojan, Virus, Worm

► Adware

ນວກໄຫວ່ານີ້.

Anti-virus approaches.

► Detection

► Identification

► Removal

► Recovery.

Subject : _____

Date : _____

Recovery from Viruses.

- clean your computer.
- disconnect internet

Preventing Virus.

- update software los.
- change password.
- enable firewall
- lock your computer
- disconnect internet
- avoid download.
- back up all of your data

Sandbox

- concept of running application client

|| សម្រាប់ app ដែលមិនអាចពិនិត្យបាន និងការងារទាំងអស់របស់វា នឹងធ្វើឡើងនៅក្នុងក្រុងការណែនាំ

• effect: ជួយបន្លឺការណែនាំ

• insert buffer

• mal - euriv - nigt និងខេត្តូវនៃការណែនាំ

• ciphertext

• zero padding antiv - itia

Chapter 10

Steganography.

❖ Steganography.

ການປິດເກີດສາມາດພາບໃຫຍ່ໄດ້ ແລະ ພາຍໃຕ້ການສໍາຜັກ ຈາກໄຕ່ມີໃຫ້ວ່າ ສາມາດສໍາຜັກໄດ້

ໄວ້ກໍລຳກ້າວກໍໄດ້ ໄກສອນໃຫ້ວ່າ ດຸຈຸກໍາມັນຍຸ

❖ Steganography & Cryptography.

- ▶ Steganography. ປິຈັນໃຫ້ວ່າ ສັງເກດມາດູ
- ▶ Cryptography. ສັງເກດໃຫ້ວ່າ ຮຶດລວມໄດ້ → ກໍາລັກ.

❖ Security and Steganography.

- ▶ Confidentiality. ວັດນາຄະນາຄົນ.
- ▶ Survivability. ການທີ່ສົມຜະລົດລັ້ນກາກອອກຖານາການ
- ▶ No detection detect ເຊັ່ນກຳນົກ.
- ▶ Visibility. ມັງໄມ້ໃຫ້ວ່າ ດຸຈຸກໍາມັນຍຸ

❖ History of Steganography.

- ▶ ສັກສົນໃຫຍ່ໄວ້ ແກ້ວຄວາມໄວ້ ໂດຍກ່າວກໍາມັນຍຸ
- ▶ ສັກໃຫຍ່ໄວ້ ແກ້ວຄວາມໄວ້ ຖ້າ ພົມປອດໄພ

World War II

- ▶ ເກືອນກັນທຳຂະໜາດ.
- ▶ "Microdot" ປົກເມືດນາໂຮງໃນກວດໝັກຂະໜາດ. ໄດ້ກົດມີກຳນົດກົດໄດ້.
- ▶ ຖ້າ ທີ່ຢູ່ຈຸດທາງໃຫ້ໃນກຽມຊົນ.

Null - Cipher

- ลีบาร์เจ็ตความก้าวหน้าของอเมริกา เนื่องจากชื่อภาษาอังกฤษ
- สำหรับงาน: หัวข้อ 2 ข้อทุกๆ ต่อ

Steganography in Text

- เว็บบลู๊ฟที่ไม่ทำให้รู้
- ข้อดีที่ไม่ทำให้รู้

XML tag steganography

 → ก้าบ bit 0
 → bit 0

Steganography in Image.

- ▶ ล้ำ
- ▶ ความซ่อน

LSB masking bit → 幻 slide 15

Steganography in Audio

- คำว่า LSB ไม่ได้ เกี่ยวกับข้อมูลในไฟล์
- สามารถใส่ไฟล์ wave ได้ แต่ไม่ต้องการเสียงทุกอย่าง

Steganography in Video

- ล้ำ logo

จุดเด่น-จุดดี ของการ์ดอัตโนมัติ คือ ไม่ใช้ภาษาไทย

Printer Steganography.

ເສັ້ນໃຈຕ່າງໆ ການຕາມແລ້ວກໍາໄລນ໌ກາງ ເຄືອງຈິງໄກນ໌ ສັບຕໍ່ຫຸນ

- ▶ ເສັ້ນໃຈຕ່າງໆ ທຳມະນີມັນຍືນ
- ▶ ເສັ້ນໃຈຕ່າງໆ ດາວ ກຳນົດ ເຊິ່ງ

Application

- ▶ ຕົ້ນກາງສິ້ງ transaction ທີ່ໄວ້ຈິງ ດາວກົນ
- ▶ ໄລນງວິໄງ້ random number = ຖົມມາເຖິງສາວິ່ງໄປໃຫຍ່ design ພະຍັດໜາກຂັ້ນ
- ▶ ໂທໄວ້ protect privacy.

Steganalysis - Methods of Detection.

▶ ອົງກວະກຸນ.

▶ ກົດຕິ

▶ detect ສັກຂະນະ: ຖົມສັກ

Chapter 10.

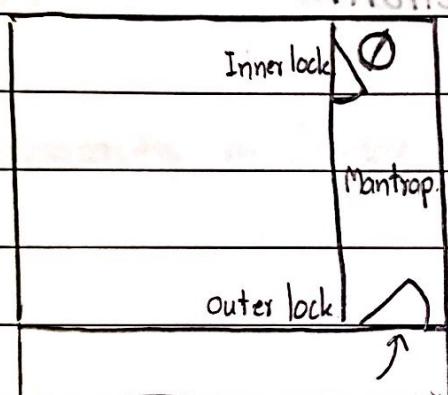
Remaining topics.

Physical Security.

- សំខាន់: រាយការណាគាយលោកស្រី.
- សំខាន់: សម្រាប់ការបង្ហាញ, សម្រាប់ការងារ.
- ដើរការសម្រាប់បង្ហាញ.

Mantrap

ការបង្ហាញ server ហាងទីនៅ ជំនាញពាក្យការ



Disaster Recovery.

► Hardware loss

► Software loss

► Data loss ដឹងរក្សាទុក្ខ ជំនាញពាក្យការ.

* ការធ្វើការ back up file នៅលើកិច្ចការ.

Privacy. ความเป็นส่วนตัวของ data.

▶ data อยู่ที่ไหน

▶ ภัยคุกคาม (threat) คืออะไร

▶ ภัยด้านข้อมูล

(good) ประโยชน์ของการเก็บรวบรวมข้อมูล

(bad) การใช้ข้อมูลโดยไม่ได้รับความยินยอม

User tracking.

▶ ทำเว็บเบราว์เซอร์บันทึก เก็บ: เก็บชื่อผู้ใช้งาน

▶ ทางเว็บไซต์บันทึกไว้ เอาไว้ใช้ต่อไป

▶ บันทึกว่าเราไปไหนมาไหนบ้าง

ทำให้เก็บข้อมูลทางการเงินไว้ช่วยเหลือ

ไม่ดีต่อกฎหมาย! หมาย: เราสามารถ track ได้ผ่านมือถือ, คอมพิวเตอร์, browser, ...

user tracking methods

▶ Cookies

▶ IP address

▶ Browser fingerprinting, : browser นี้มีลักษณะเด่นๆ อย่างไรบ้าง

Privacy Risks ภัยคุกคาม: Privacy.

● ผู้คน track ตัว

● log data ตัว

● Spyware program.

● หัวข้อมูลใน Search engine.

● Pokemon Go.

Pokemon Go

▪ = เก็บข้อมูล location, storage, camera

Android : เข้าถึง USB storage, contacts, network connection ตัว

iPhone : เข้าถึง google account ตัว

❖ Quality of Service. (QoS)

► Service Level Agreement (SLA)

តើលក្ខណៈនីងក្នុងការប្រើការសំរាប់សេវាដែល មាត្រាទំនួន។ (Standard)

► Example QoS parameter.

- រាយការសំខាន់នៅក្នុងការប្រើប្រាស់។

- time out

- Throughput នៃ ការអាជីវកម្ម។

- ចំណាំគិត។

- error rate: នៅក្នុងការប្រើប្រាស់។

- និរនោះក្នុងការប្រើប្រាស់។

► QoS Issues

ទៅលើសម្រាប់ការប្រើប្រាស់។ សំរាប់សេវាដែល មាត្រាទំនួន។

ផែនធ៌៖ តើលក្ខណៈនីងក្នុងការប្រើប្រាស់។

❖ Performance Issues

► resource នៃ ការអាជីវកម្ម។

ការអាជីវកម្ម OK មឺន។

resource brance មឿន, នៅពេលការប្រើប្រាស់។

ចំណាំការប្រើប្រាស់ និង performance.

Potential pitfalls

- ចំណាំទូទៅ: នៅ (វត្ថុកម្មភាព) → Sample size.

- representative → data នៃ វត្ថុកម្មភាពក្នុងក្នុងការប្រើប្រាស់។

- bias results → ទិន្នន័យ: ការអាជីវកម្ម។

វត្ថុកម្មភាព នឹងការប្រើប្រាស់។ នៅពេលមិនមែន: ឱ្យ ការប្រើប្រាស់ និង ការអាជីវកម្ម។

✿ Network management

► Three principle components.

- Managing entity : user
- Managed devices : spec խաղօղակներ
- A network management protocol : դրա performance քայլություն (policy)

► Առաջին պատճեններ. ~

► Network vulnerabilities Դժվար հայտնաբերելու համար.

- Առ և ՏՀԱ.
- security հիմքածող համակարգ firewall, ՊՏ և DMZ.
- Network core security → switch, ԲԿ, physical

► Defense in Depth : օժանական համակարգ առաջախօսություն հիմքածող համակարգ.

► Գրադարանի համակարգ համապատասխան համակարգերներ.

✿ 4-Step process.

► Acquisition. Լարձակ, լրացնելու համար կամ գնացնելու համար.

► Identification. Հաշվությունների համար.

► Evaluation Երրորդական, 9 մակարդակության մասնակիություն.

► Presentation. Հաշվությունների պատճենագրությունը կամ պատճենագրությունը.

Present

Subject : _____

Date : _____

1. Hack WiFi WEP

WEP : វាគ់តិចខ្លួនការបោះឆ្នោត ការពារនៃការបង្កើតឱ្យសម្រាប់អេដ្ឋុក
នៅក្នុងការការពារនៃការបង្កើតឱ្យសម្រាប់អេដ្ឋុក និងការបង្កើតឱ្យសម្រាប់
ការបង្កើតឱ្យសម្រាប់ការបង្កើតឱ្យសម្រាប់ការបង្កើតឱ្យសម្រាប់ការបង្កើតឱ្យសម្រាប់
ការបង្កើតឱ្យសម្រាប់ការបង្កើតឱ្យសម្រាប់ការបង្កើតឱ្យសម្រាប់ការបង្កើតឱ្យសម្រាប់

WPA : ជូនការបោះឆ្នោត ការពារនៃការបង្កើតឱ្យសម្រាប់ការបង្កើតឱ្យសម្រាប់
នៅក្នុងការបង្កើតឱ្យសម្រាប់ការបង្កើតឱ្យសម្រាប់ការបង្កើតឱ្យសម្រាប់ការបង្កើតឱ្យសម្រាប់

WPA2 : គ្មានធម្មានដឹងការបោះឆ្នោត ការពារនៃការបង្កើតឱ្យសម្រាប់ការបង្កើតឱ្យសម្រាប់

► របៀបង្កើតឱ្យសម្រាប់

ប្រព័ន្ធសាស្ត្រ wireless ដើម្បីការបង្កើតឱ្យសម្រាប់

2. Hack Any Android Phone

► របៀបង្កើតឱ្យសម្រាប់

អាមេរិកាតិទាំងអស់រាយការណ៍ file.apk និង ហ៊ែស៉ីមិតិណុញ្ញនាមរបៀប

3. DNS spoofing

► **DNS spoofing** នាំរាយការណ៍សម្រាប់ DNS ផ្លូវការតែ IP address ដែលមានតម្លៃជាទុក
ខែប្រាំបី នាំរាយការណ៍សម្រាប់ការបង្កើតឱ្យសម្រាប់ 2 message តែ request, reply ទៅបានការបង្កើតឱ្យសម្រាប់
ទីផ្សារទី១: តែ request ដើម្បី ID ដែលត្រូវការពារនៃ DNS server ទៅ DNS server
ទីផ្សារទី២: តែ reply នៅ ID ដែលការពារឡើង Tofu Hacker ទៅបានការបង្កើតឱ្យសម្រាប់ request នៅ
ទីផ្សារទី២ ទៅបានការបង្កើតឱ្យសម្រាប់ DNS server ទៅបាន

► រាយការណ៍នេះ ការបង្កើតឱ្យសម្រាប់

- ចូលរួម Windows Defender របស់យើង របស់យើង ក្នុងការបង្កើតឱ្យសម្រាប់ DNS នៃ web.

- ពិនិត្យការពារនៃ DNS server ដើម្បីមានការបង្កើតឱ្យសម្រាប់

- ដូចតារាពន្លឹងសម្រាប់ការបង្កើតឱ្យសម្រាប់ hosts ឬការពារនៃការបង្កើតឱ្យសម្រាប់ Domain name
ក្នុងកម្មិតិរបាយការណ៍

4. Facebook Message Injection.

5. Hack Gmail account & password

b. Hack gmail

ព័ត៌មានអ៊ីមែលរបស់ខ្លួន និងអ៊ីមែលទាំងអស់គ្មាន និងទូរសព្ទ នៅក្នុង Gmail

7. Hacking windows using

Metaploit framework: កម្រិតម៉ែនការីមិនការណ៍វានៅក្នុងការងារជាបីនុយ្យូរបាយពេញ ទៀត វិច្ឆិក reverse TCP payload នូវសារសំណើអាជីវកម្ម executable file ក្នុងការងារដែលវិញ្ញាបនកិត្យ និងការងារដែលវិញ្ញាបនកិត្យ payload នូវសារសំណើអាជីវកម្មដែលបានចាត់បន្ថែម ការងារនេះនឹងការងារបានរាយការណ៍ឡើង នូវការងារបានរាយការណ៍ឡើង command line.

8. Hack SSH.

◀ გასტრო

▶ ចំណាំ

ខ្លួនកំណត់ទូទាត់លើ password នៅរឿង ដែលកំណត់ឡើងនៅក្នុងកិច្ចការណ៍ ពេលវេលា បាន។

9. DDoS

ເນື້ອງໄວ່ຈະຕີຄວາມພົດກວນໃຈ: ທີ່ກຳທົບເຫັນອາຍໃຫ້ໂປ່ສໍາກຳໜ້າ server ຂູ້ຕົກ ເຖິງກົງເລີນ
ກົມໄມ່ ກົມແກຕີເຫັນໃຈ