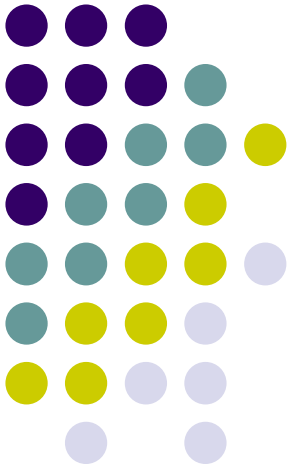
ຄະນະວິທະຍາສາດທຳມະຊາດ
ພາກວິຊາ ວິທະຍາສາດຄອມພິວເຕີ

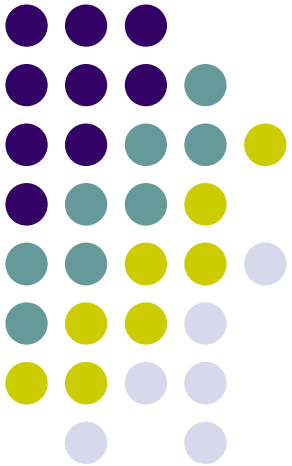
ຄວາມປອດໄພເວບໄຊ
(Web Security)

ສອນໂດຍ: ອຈ ເພັດ ສອນວິໄລ
ມືຖື: 020 58390300
ອີເມວ: p.sonevilay@nuol.edu.la

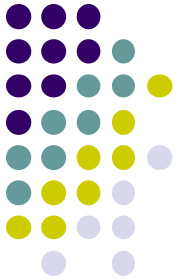


ບົດທີ2

Information Gathering Techniques

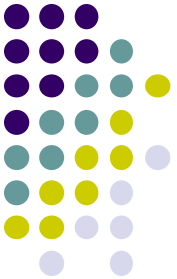


ເນື້ອໃນໂດຍລວມ



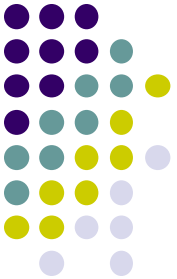
- Information Gathering ເບື້ອງຕົ້ນ
- Information Gathering Techniques
- Enumerating Domains, Files, and Resources
- ເຄື່ອງມືທີ່ໃຊ້ໃນການສະແດງຂໍ້ມູນ
- ເວບໄຊ໌ທີ່ໃຊ້ໃນການສະແດງຂໍ້ມູນ

Information Gathering ເບື້ອງຕົ້ນ



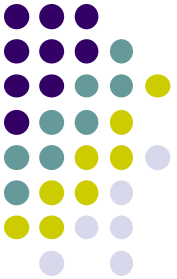
- Information Gathering ເປັນການພະຍາມສຳຫຼວດແວດລ້ອມ ແລະ ສະແດງຂໍ້ມູນຕ່າງໆຂອງເປົ້າໝາຍທີ່ຈະໂຈມຕີ.
- ຂໍ້ມູນທີ່ໄດ້ຈາກການສຳຫຼວດເປົ້າໝາຍ ເຊັ່ນວ່າ: ໝາຍເລກ ports ທີ່ນຳໃຊ້, ໂປຣແກຣມ ຫຼື services ທີ່ເຮັດວຽກຢູ່, ໂປຣແກຣມນຳໃຊ້ທີ່ບໍ່ໄດ້ມີລະບົບການຢືນຢັນຜູ້ໃຊ້ ຫຼື ນຳໃຊ້ລະຫັດຜ່ານທີ່ງ່າຍດາຍ.

Information Gathering Techniques



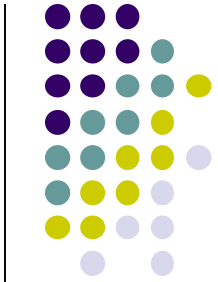
- Information Gathering Techniques ມີ 2 ແບບຄື:
  - Active techniques ເປັນການເຊື່ອມຕໍ່ໄປຍັງເຄື່ອງເປົ້າໝາຍທີ່ຈະໂຈມຕີ ເພື່ອສະແດງຂໍ້ມູນຕ່າງໆທີ່ກ່ຽວຂ້ອງ ເຊັ່ນ ວ່າ: ໝາຍເລກ Port, ໄຟລ໌ຂໍ້ມູນ ແລະ ອື່ນໆ.
  - Passive techniques ເປັນການນຳໃຊ້ເຄື່ອງມື ແລະ ເວບໄຊ໌ໃນການສະແດງຂໍ້ມູນທີ່ກ່ຽວຂ້ອງກັບເຄື່ອງເປົ້າໝາຍ, ຊຶ່ງເຮົາບໍ່ໄດ້ເຊື່ອມຕໍ່ໄປຍັງເປົ້າໝາຍໂດຍກົງ.

Enumerating Domains, Files, and Resources



- Enumerating Domains, Files, and Resources ເປັນການສຳຫຼວດຂໍ້ມູນດູເມນ, ໄຟລ໌ຂໍ້ມູນ ແລະ ຂໍ້ມູນທີ່ກ່ຽວຂ່ອງຕ່າງໆ ໂດຍນຳໃຊ້ທັງແບບ Active ແລະ Passive Techniques.
- ເຄື່ອງມືທີ່ນຳໃຊ້ ມີດັ່ງລຸ່ມນີ້:
  - Fierce
  - theHarvester
  - SubBrute
  - CeWL – Custom Word List Generator

Enumerating Domains, Files, and Resources



- ເຄື່ອງມືທີ່ນຳໃຊ້ (ຕໍ່)
  - DirBuster
  - WhatWeb
  - Maltego
  - **WHOIS Database Lookup**

ເຄື່ອງມືທີ່ໃຊ້ໃນການສະແດງຂໍ້ມູນ

- Fierce

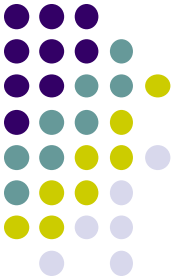
ຕົວຢ່າງ: fierce -dns google.com

ເຄື່ອງມືທີ່ໃຊ້ໃນການສະແດງຂໍ້ມູນ

- theHarvester

ຕົວຢ່າງ: theharvester -d google.com -b google

ເຄື່ອງມືທີ່ໃຊ້ໃນການສະແດງຂໍ້ມູນ

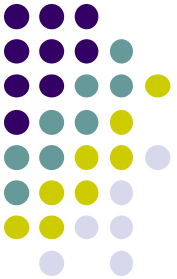


- SubBrute

https://github.com/TheRook/subbrute

ຕົວຢ່າງ: ./subbrute.py google.com

ເຄື່ອງມືທີ່ໃຊ້ໃນການສະແດງຂໍ້ມູນ



- CeWL

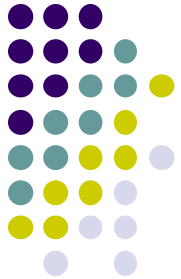
https://digi.ninja/projects/cewl.php#download

ຕົວຢ່າງ: ./cewl target.com

ຂໍ້ມູນອ້າງອີງ

[1] J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan. Improving Web Application Security, Microsoft Corporation, 2013

[2] Information Gethering . Ref: https://secur1tyadvisory.wordpress.com/2015/07/10/information-gathering-first-step-of-hacking/



ຖາມ ແລະ ຕອບ

ຂອບໃຈ