



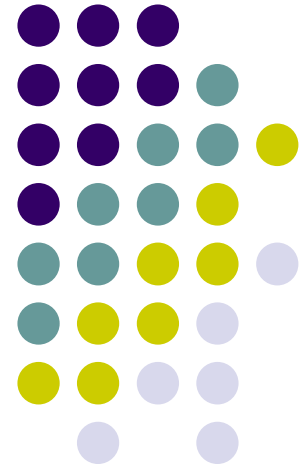
ຄະນະວິທະຍາສາດທຳມະຊາດ
ພາກວິຊາ ວິທະຍາສາດຄອມພິວເຕີ

ຄວາມປອດໄພເວບໄຊ້ (Web Security)

ສອນໂດຍ: ອຈ ເພັດ ສອນວິໄລ

ມືຖື: 020 58390300

ອີເມວ: p.sonevilay@nuol.edu.la



ບົດທີ3

ໄພຄຸກຄາມ ແລະ ວິທີການຈັດການ(Threats and Countermeasures)

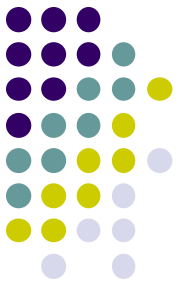




ເນື້ອໃນໂດຍລວມ

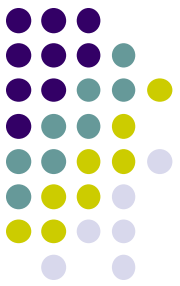
- ສະເໜີເບື້ອງຕົ້ນ
- ວິທີການພື້ນຖານການປຸກໂຈມຕີ(Attacking methodology)
- ໄພຄຸກຄາມເຄື່ອນຂ້າຍ ແລະ ວິທີຈັດການ(Network Threats and Countermeasurement)
- ໄພຄຸກຄາມຄອມພິວເຕີ ແລະ ວິທີຈັດການ(Host Threats and Countermeasures)
- ໄພຄຸກຄາມທາງໂປຣແກຣມ(Application Threats)

ສະເໜີເບື້ອງຕົ້ນ



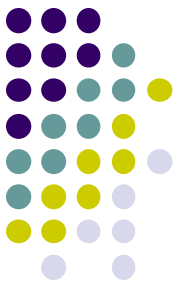
- ເມື່ອມີການນຳໃຊ້ຄຸນລັກສະນະຄວາມປອດໄພເຂົ້າໃນການອອກແບບ, ສ້າງ ແລະ ນຳໃຊ້ ໂປຣແກຣມ ມັນຈະຊ່ວຍໃຫ້ເຂົ້າໃຈເຖິງແນວຄວາມຄິດ ແລະ ວິທີການຂອງຜູ້ບຸກໂຈມຕີ(Attacker), ຊຶ່ງຈະເຮັດໃຫ້ຜູ້ພັດທະນາຮູ້ຈັກວິທີປ້ອງກັນ ແລະ ຈັດການກັບໄພຄຸກຄາມດັ່ງກ່າວ.
- ຜູ້ບຸກໂຈມຕີ(Attacker) ຈະຄຸກຄາມລະບົບດ້ວຍການບຸກໂຈມຕີເຄືອຄ່າຍ(Network), ຄອມພິວເຕີ(Host) ແລະ ໂປຣແກຣມ(Application).

ວິທີການພື້ນຖານການບຸກໂຈມຕີ(Attacking methodology)

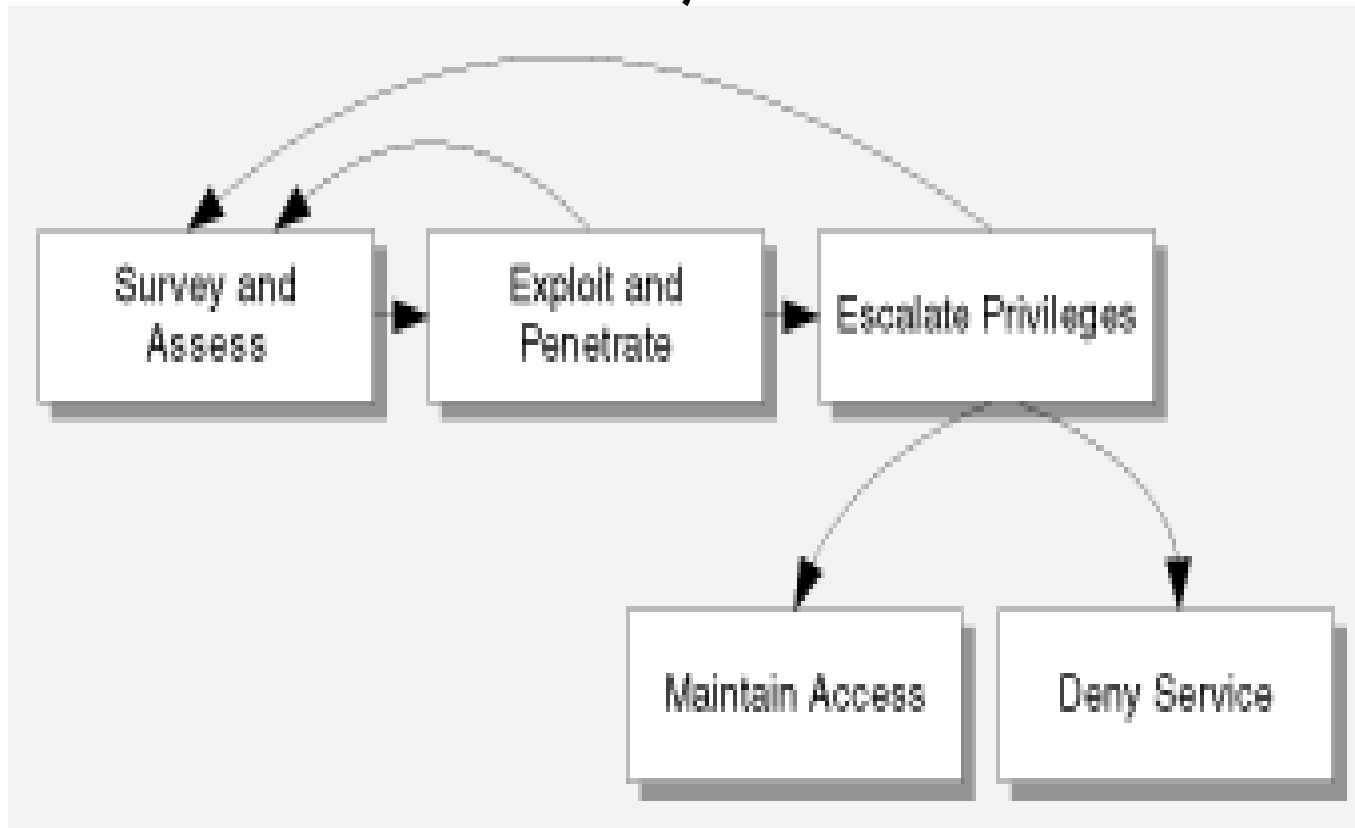


- ຂັ້ນຕອນການບຸກໂຈມຕີມີດັ່ງລຸ່ມນີ້:
 - ການສຳຫຼວດ ແລະ ປະເມີນ(Survey and Assess)
 - ການເຈາະລະບົບ ແລະ ນຳໃຊ້ຜົນໄດ້ຮັບ(Exploit and Penetrate)
 - ການຂະຫຍາຍສິດທິ(Escalate Privileges)
 - ການເຈາະຈຸດອ່ອນ(Maintain Access)
 - ການຍົກເລີກບໍລິການ(Deny Services)

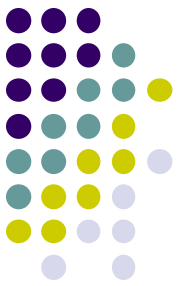
ວິທີການພື້ນຖານການບຸກໂຈມຕີ(Attacking methodology)



- ສະແດງຂັ້ນຕອນການບຸກໂຈມຕີ

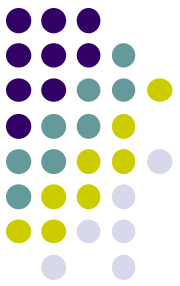


ວິທີການພື້ນຖານການບຸກໂຈມຕີ(Attacking methodology)



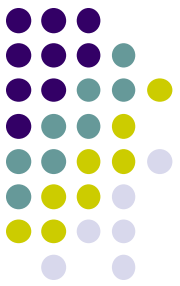
- ການສຳຫຼວດ ແລະ ປະເມີນ(Survey and Assess)
- ການສຳຫຼວດ ແລະ ປະເມີນເປົ້າໝາຍທີ່ເປັນໄປໄດ້ຕໍ່ການບຸກໂຈມຕີ ຈະເຮັດເປັນວົງຮອບຈົນກວ່າຈະພົບຈຸດອ່ອນ ຫຼື ຊ່ອງໂວຂອງໂປຣແກຣມ.
- ພາຍຫຼັງທີ່ໄດ້ຂໍ້ມູນຊ່ອງໂວແລ້ວຈະນຳໃຊ້ຂໍ້ມູນດັ່ງກ່າວເພື່ອວາງແຜນການບຸກໂຈມຕີ.
- ຕົວຢ່າງ: ຜູ້ບຸກໂຈມຕີສຳຫຼວດຈຸດອ່ອນ ຫຼື ຊ່ອງໂວ ແບບ cross-site scripting (XSS) ຂອງເວບ, ຖ້າພົບຈຸດອ່ອນຈະສະແດງຂໍ້ຜິດພາດອອກມາ ແລະ ຜູ້ບຸກໂຈມຕີຈະນຳໃຊ້ຂໍ້ມູນເພື່ອວາງແຜນການບຸກໂຈມຕີ.

ວິທີການພື້ນຖານການປຸກໂຈມຕີ(Attacking methodology)



- ການເຈາະລະບົບ ແລະ ນຳໃຊ້ຜົນໄດ້ຮັບ(Exploit and Penetrate)
 - ພາຍຫຼັງໄດ້ຂໍ້ມູນຈຸດອ່ອນເປົ້າໝາຍແລ້ວຈະທຳການເຈາະເຂົ້າສູ່ລະບົບຕາມແຜນທີ່ວາງໄວ້.
 - ຖ້າເຄື່ອຂ່າຍ ແລະ ເຄື່ອງເຊີເວີມີຄວາມປອດໄພແໜ້ນໜາດີແລ້ວ, ໂປຣແກຣມຈະເປັນເປົ້າໝາຍໃນການເຂົ້າສູ່ລະບົບ.
 - ຕົວຢ່າງ: ການໂຈມຕີເຂົ້າສູ່ລະບົບຜ່ານໜ້າໂປຣແກຣມເຂົ້າສູ່ລະບົບຂອງຜູ້ໃຊ້(Login Page) ຫຼື ໜ້າທີ່ບໍ່ຕ້ອງການມີການຢືນຢັນຜູ້ໃຊ້(Authentication).

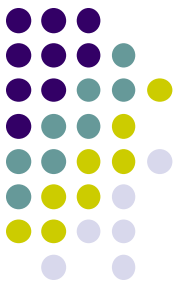
ວິທີການພື້ນຖານການປຸກໂຈມຕີ(Attacking methodology)



■ ການຂະຫຍາຍສິດທິ(Escalate Privileges)

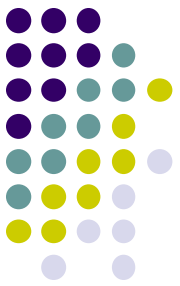
- ພາຍຸຫຼັງເຂົ້າສູ່ລະບົບໄດ້ແລ້ວ, ຜູ້ປຸກໂຈມຕີຈະນຳໃຊ້ສິດທິຂອງຜູ້ໃຊ້ທີ່ຢູ່ໃນກຸ່ມດຽວກັນເພື່ອສະແດງຂໍ້ມູນຂອງກຸ່ມຜູ້ໃຊ້ທີ່ເປັນລະດັບຜູ້ບໍລິຫານ(Administrator).
- ຕົວຢ່າງ: ການໂຈມຕີເຂົ້າສູ່ລະບົບຜ່ານໜ້າໂປຣແກຣມເຂົ້າສູ່ລະບົບຂອງຜູ້ໃຊ້(Login Page) ຫຼື ໜ້າທີ່ບໍ່ຕ້ອງການມີການຢືນຢັນຜູ້ໃຊ້(Authentication).
- ການເຂົ້າເຖິງໄຟລ /etc/passwd ຂອງລະບົບ Unix ໂດຍການເຂົ້າຈາກຜູ້ໃຊ້ ໃດໜຶ່ງຂອງ FTP server. ຈຸດອ່ອນກໍຄືນຳໃຊ້ລະຫັດຜ່ານງ່າຍດາຍ ເຮັດໃຫ້ເດົາໄດ້ງ່າຍ.

ວິທີການພື້ນຖານການບຸກໂຈມຕີ(Attacking methodology)



- ການເຈາະຈຸດອ່ອນ(Maintain Access)
 - ພາຍຫຼັງເຂົ້າສູ່ລະບົບໄດ້ແລ້ວ, ຜູ້ບຸກໂຈມຕີຈະວາງແຜນການເຂົ້າເຖິງຂໍ້ມູນໂດຍນຳໃຊ້ໂປຣແກຣມ Back-door ຫຼື ໃຊ້ account ທີ່ບໍ່ມີຄວາມປອດທີ່ມີຢູ່ໃນລະບົບ. ວິທີການຈະໃຊ້ການ account ດັ່ງກ່າວເຂົ້າໄປລຶບຂໍ້ມູນການຕິດຕາມຜູ້ໃຊ້(Clear logs), ເຊື່ອງເຄື່ອງມື ເຊັ່ນວ່າ: ເຄື່ອງມືການເກັບກຳການກວດສອບສິດຜູ້ໃຊ້(audit logs) ຊຶ່ງເປັນເປົ້າໝາຍຫຼັກຂອງຜູ້ບຸກໂຈມຕີ.

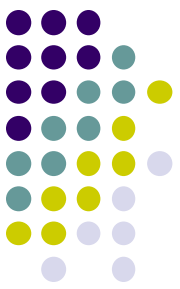
ວິທີການພື້ນຖານການປຸກໂຈມຕີ(Attacking methodology)



■ ການຍົກເລີກບໍລິການ(Deny Services)

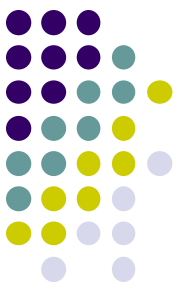
- ຜູ້ປຸກໂຈມຕີທີ່ບໍ່ສາມາດເຂົ້າເຖິງຂໍ້ມູນໄດ້ສໍາເລັດໂດຍກົງຈະໃຊ້ການໂຈມຕີແບບຍົກເລີກການບໍລິການໃດໜຶ່ງໃນລະບົບ, ຊຶ່ງຈະເຮັດລະບົບປະຕິເສດການເຂົ້າເຖິງຂໍ້ມູນຂອງຜູ້ຄົນອື່ນໆ.
- ຕົວຢ່າງ: ການໂຈມຕີແບບ SYN flood ໂດຍຜູ້ປຸກໂຈມຕີຈະນໍາໃຊ້ໂປຣແກຣມສົ່ງຂໍ້ມູນລົບກວນລະບົບຜ່ານຊ່ອງທາງການສື່ສານເຄືອຂ່າຍ (Flood of TCP SYN) ເພື່ອໃຫ້ການເຊື່ອມຕໍ່ກັບໂປຣແກຣມຜ່ານເຄືອຂ່າຍເກີດການລໍຖ້າເປັນຄົວຍາວຢູ່ໃນເຄືອເຊີເວີ. ບັນຫາດັ່ງກ່າວກໍ່ໃຫ້ເກີດການຍົກເລີກການບໍລິການຢູ່ໃນລະບົບ.

ໄພຄຸກຄາມເຄື່ອນຍ້າຍ ແລະ ວິທີປ້ອງກັນ (Network Threats and Countermeasurement)



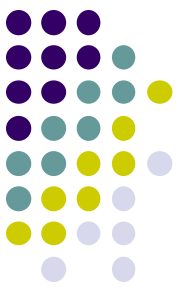
- ຄວາມປອດໄພຂອງເຄື່ອນຍ້າຍປະກອບດ້ວຍອຸປະກອນ routers, firewalls, ແລະ switches. ອຸປະກອນດັ່ງກ່າວ ຈະເປັນໂຕປ້ອງກັນການບຸກໂຈມຕີຜ່ານທາງເຄື່ອນຍ້າຍ ເຂົ້າຫາເຄື່ອງເຊີເວີ ແລະ ໂປຣແກຣມ.
- ໄພຄຸກຄາມເຄື່ອນຍ້າຍປະກອບມີດັ່ງນີ້:
 - ການນຳຮອຍຂໍ້ມູນ(Information gathering)
 - ການດັກຈັບຂໍ້ມູນ(Sniffing)
 - ການປອມໂຕ(Spoofing)
 - ການໂຈມຕີໂດຍຄົນກາງ(Session hijacking)
 - ການປະຕິເສດບໍລິການ(Denial of service)

ເພື່ອກຳລັງຄວາມເຄອນຂາຍ ແລະ ວິທະຍາສາດ (Network Threats and Countermeasurement)



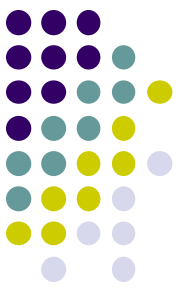
- ການນຳຮອຍຂໍ້ມູນ (Information gathering)
 - ການນຳຮອຍເປັນຊອກຫາຂໍ້ມູນອຸປະກອນເຄື່ອນຂ່າຍຕ່າງໆເພື່ອໃຫ້ໄດ້ຂໍ້ມູນເປົ້າໝາຍຂອງອຸປະກອນທີ່ຈະມາປະກອບການບຸກໂຈມຕີ ເຊັ່ນວ່າ: ຊື່ອຸປະກອນ, ຊື່ເຄື່ອງຄອມພິວເຕີ ແລະ ຂໍ້ມູນອື່ນໆ.
- ການປ້ອງກັນ.
 - ອຸປະກອນ Router ຕ້ອງມີການຕັ້ງຄ່າຢ່າງປອດຈາກການແກະຮອຍ.
 - ລະບົບປະຕິບັດການຕ້ອງມີການຕັ້ງຄ່າດ້ວຍການປິດໂຕກາງການສື່ສານ (Protocol) ຫຼື ຊ່ອງທາງການສື່ສານ (Ports) ທີ່ບໍ່ໄດ້ໃຊ້ (ເປີດ Firewall).

ເພື່ອກຳລັງເຄື່ອນຂ້າງ ແລະ ວິທີການ (Network Threats and Countermeasurement)



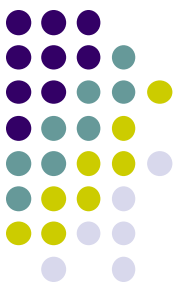
- ການດັກຈັບຂໍ້ມູນ(Sniffing)
 - ການດັກຈັບຂໍ້ມູນໝາຍເຖິງການສອດແນມທີ່ເພື່ອເບິ່ງຂໍ້ມູນທີ່ສົ່ງຜ່ານເຄື່ອນຂ້າງ.
 - ຕົວຢ່າງ: ການດັກອ່ານຂໍ້ມູນທີ່ສົ່ງຜ່ານເຄື່ອນຂ້າງ, ການອ່ານໄຟລຂໍ້ມູນຢູ່ໃນລະບົບ, ແລະ ການຕິດຕາມຂໍ້ມູນທີ່ສົ່ງຜ່ານສາຍລະບົບ(Wiretapping).
- ການປ້ອງກັນ.
 - ຂໍ້ມູນຕ້ອງເຂົ້າລະຫັດ(Encryption) ເຊັ່ນວ່າ: ນຳໃຊ້ SSL ແລະ IPsec (Internet Protocol Security)

ເພື່ອກຳລັງເຄື່ອນຂ້າງ ແລະ ວິທີການ (Network Threats and Countermeasurement)



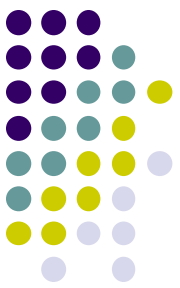
- ການປອມໂຕ(Spoofing)
 - ການປອມໂຕໝາຍເຖິງການເຊື່ອງຊ້ອນໂຕເອງຢູ່ໃນລະບົບເຄື່ອນຂ້າງເພື່ອປອມໂຕໃຫ້ອີກຝ່າຍໜຶ່ງເຂົ້າໃຈວ່າເປັນຜູ້ໃຊ້ຈິງຢູ່ໃນລະບົບ.
 - ຕົວຢ່າງ: ຜູ້ໃຊ້ຕ້ອງການເຂົ້າສູ່ລະບົບຜ່ານເຄື່ອນຂ້າງອື່ນເຕີເນັດ, ແຕ່ມີການຕົວະໃຫ້ເຂົ້າສູ່ລະບົບອື່ນ ຊຶ່ງຜູ້ໃຊ້ຄົນນັ້ນຄິດວ່າເປັນລະບົບທີ່ຕົນເອງຕ້ອງການເຂົ້າສູ່ຈິງ.
- ການປ້ອງກັນ.
 - ນຳໃຊ້ການຢືນຢັນຜູ້ໃຊ້(Authentication) ເພື່ອກັນກອງແລະ ພິສູດຜູ້ໃຊ້.

ໄພຄຸກຄາມເຄືອຂ່າຍ ແລະ ວິທີປ້ອງກັນ (Network Threats and Countermeasurement)



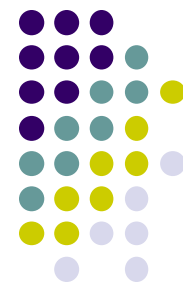
- ການໂຈມຕີໂດຍຄົນກາງ(Session hijacking)
 - ການໂຈມຕີແບບຄົນກາງເປັນການພະຍາຍາມທີ່ຈະໃຊ້ບັນຊີຜູ້ໃຊ້ (User accounts) ທີ່ຖືກຕ້ອງເຂົ້າສູ່ລະບົບ.
 - ການໂຈມຕີແບບຄົນກາງສາມາດເຮັດໄດ້ໂດຍການລັກເອົາລະຫັດຂອງບັນຊີຜູ້ໃຊ້(sessionID)ທີ່ມີການສົ່ງຜ່ານ Cookie ແລະ ນຳມາໃຊ້ເຂົ້າສູ່ລະບົບ.
 - ຕົວຢ່າງ: ການລັກເອົາລະຫັດຈາກເຄື່ອງຜູ້ໃຊ້ໃດໜຶ່ງແລ້ວມາໃຊ້ການການເຂົ້າສູ່ລະບົບດ້ວຍການໃຊ້ SQL-Injection ດັ່ງນີ້: abc' or 1=1-- ກໍສາມາດເຂົ້າສູ່ລະບົບດ້ວຍຜູ້ໃຊ້ທີ່ຖືກຕ້ອງ.
- ວິທີປ້ອງກັນ.
 - ເຂົ້າລະຫັດຂໍ້ມູນ(Session) ແລະ ກວດສອບຂໍ້ມູນໃນການສື່ສານລະຫວ່າງ ຜູ້ໃຊ້ ແລະ ເຊີເວີ

ເພື່ອກຳລັງເຄື່ອນຂ້າງ ແລະ ວິໄຈດການ (Network Threats and Countermeasurement)



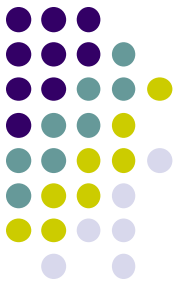
- ການປະຕິເສດບໍລິການ(Denial of service)
 - ການປະຕິເສດບໍລິການເປັນການໂຈມຕີເຄື່ອງເຊີເວີເພື່ອບໍ່ໃຫ້ບໍລິການຊັບພະຍາກອນໃຫ້ກັບຜູ້ໃຊ້ໄດ້, ເຊັ່ນວ່າ: ການໂຈມຕີແບບກະຈາຍ (DDoS: Distributed Denial of Service) ກໍ່ເປັນການໂຈມຕີເຄື່ອງເຊີເວີໃຫ້ເຊີປະຕິເສດການໃຫ້ບໍລິການ.
 - ວິທີໂຈມຕີແບບກະຈາຍ ນີ້ຜູ້ໂຈມຕີອາດຈະໃຊ້ການໃຫ້ດາວໂລດໂປຣແກຣມຜ່ານທາງອິນເຕີເນັດ ແລະ ແນບໂປຣແກຣມປະເພດ Malware ຫຼື Trojan horse ໄປນຳໄຟລ ແລະ ເມື່ອເຄື່ອງທີ່ຕິດຈະເອີ້ນວ່າໂປຣແກຣມຜິດິບ(Zombie).
- ການປ້ອງກັນ
 - ນຳໃຊ້ລະບົບກວດສອບການນຳໃຊ້ເຄື່ອຂ້າຍ(Network intrusion detection system)

ໄພຄຸກຄາມຄອມພິວເຕີ ແລະ ວິທີຈັດການ(Host Threats and Countermeasures)



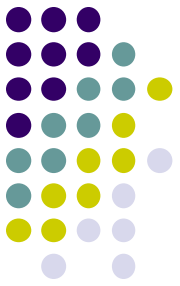
- ໄພຄຸກຄາມຄອມພິວເຕີໝາຍເຖິງການເຂົ້າເຖິງລະບົບຊອບແວທີ່ຕິດຕັ້ງຢູ່ໃນເຄື່ອງໂດຍກົງ, ເຊັ່ນວ່າ: ລະບົບປະຕິບັດການ Windows server 2003, ເວບເຊີເວີ Internet Information Services (IIS), .NET Framework, ແລະ ໂປຣແກຣມຖານຂໍ້ມູນ SQL Server ຂຶ້ນກັບການຕັ້ງຄ່າຄວາມປອດໄພຂອງເຄື່ອງເຊີເວີ.
- ລຳດັບໄພຄຸກຄາມຂອງເຄື່ອງເຊີເວີ
 - Viruses, Trojan horses, ແລະ worms
 - Footprinting
 - Password cracking

ໄພຄຸກຄາມຄອມພິວເຕີ ແລະ ວິທີຈັດການ(Host Threats and Countermeasures)



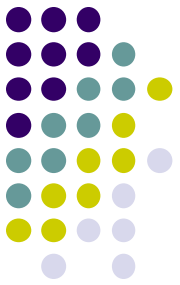
- ລຳດັບໄພຄຸກຄາມຂອງເຄື່ອງເຊີເວີ(ຕໍ່)
 - Denial of service
 - Arbitrary code execution
 - Unauthorized access

ໄພຄຸກຄາມຄອມພິວເຕີ ແລະ ວິທີຈັດການ(Host Threats and Countermeasures)



- **Viruses, Trojan horses, ແລະ worms**
 - Viruses ເປັນໂປຣແກຣມທີ່ອອກແບບມາເພື່ອລົບກວນ ແລະ ສ້າງຄວາມເສຍຫາຍໃຫ້ກັບລະບົບປະຕິບັດການ ແລະ ໂປຣແກຣມນຳໃຊ້.
 - Trojan horses ຄ້າຍຄືກັນກັບໄວຣັດແຕ່ຈະເຊື່ອງຄຳສັ່ງທີ່ທຳລາຍໄຟລູກີ ລະບົບໄວ້ທາງໃນ ແລະ ມັນຈະເຮັດວຽກເມື່ອມີການເອີ້ນໃຊ້ໂປຣແກຣມ.
 - Worms ຄ້າຍຄືກັນກັບ Trojan horses ແຕ່ຈະເຮັດວຽກດ້ວຍການກະຈາຍໂຕເອງຈາກເຄື່ອງເຊີເວີໜຶ່ງໄປຍັງອີກເຊີອີນຢູ່ໃນເຄືອຂ່າຍ.
- **ການປ້ອງກັນ**
 - ຕ້ອງປັບປຸງ Service Pack ຂອງລະບົບປະຕິບັດການ ແລະ ຊອບແວ patches.
 - ຕິດຕັ້ງ Firewall ເພື່ອປິດ Port ແລະ ບໍລິການທີ່ບໍ່ໄດ້ໃຊ້.
 - ປັບປຸງການຕັ້ງຄ່າຄວາມປອດໄພເຊີເວີທີ່ມີຈຸດອ່ອນ.

ໄພຄຸກຄາມຄອມພິວເຕີ ແລະ ວິທີຈັດການ(Host Threats and Countermeasures)



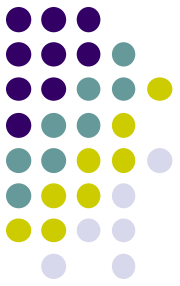
■ Footprinting

- Footprinting ເປັນການແກະຮອຍເອົາຂໍ້ມູນເພື່ອປະກອບການໂຈມຕີ ເຊັ່ນວ່າ: port scans, ping sweeps, ແລະ ການສະແດງຂໍ້ມູນ NetBIOS.
- ປະເພດຂໍ້ມູນທີ່ເປັນຈຸດອ່ອນໃນການແກະຮອຍ ເຊັ່ນວ່າ: ຂໍ້ມູນບັນຊີຜູ້ໃຊ້, ລະບົບປະຕິບັດການ, ລຸ້ນຂອງຊອບແວ ແລະ ຖານຂໍ້ມູນ.

■ ການປ້ອງກັນ

- ປິດ Protocol ທີ່ບໍ່ໄດ້ໃຊ້
- ນຳໃຊ້ Firewall ປ້ອງກັນ Port ຢ່າງເໝາະສົມ
- ຕັ້ງຄ່າເວບເຊີເວີເພື່ອປ້ອງກັນການສະແດງຂໍ້ຜິດພາດ

ໄພຄຸກຄາມຄອມພິວເຕີ ແລະ ວິທີຈັດການ(Host Threats and Countermeasures)



- **Password cracking**

- ຖ້າຜູ້ໂຈມຕີບໍ່ສາມາດສ້າງການເຊື່ອມຕໍ່ແບບ anonymous ກັບເຊີເວີສໍາເລັດຈະໃຊ້ການເຊື່ອມຕໍ່ແບບ authenticated. ຖ້າມີການກຳນົດບັນຊີຜູ້ໃຊ້ແບບອັດຕະໂນມັດ(Default) ຈະເປັນຈຸດອ່ອນສໍາລັບການແກະລະຫັດຜ່ານ. ຖ້າກຳນົດໃຫ້ລະຫັດຜ່ານເປົ່າຫວ່າງ ຫຼື ງ່າຍໂພດຈະເປັນຈຸດອ່ອນສໍາລັບການແກະລະບົບ.

- **ການປ້ອງກັນ**

- ກຳນົດລະຫັດຜ່ານໃຫ້ປອດໄພ(Strong password)
- ກຳນົດຄັ້ງໃນການປ້ອນລະຫັດຜ່ານເພື່ອບໍ່ໃຫ້ພະຍາຍາມເດົາໄດ້ຫຼາຍຄັ້ງ
- ຫ້າມບໍ່ໃຫ້ໃຊ້ຕັ້ງຊື່ຜູ້ໃຊ້ແບບອັດຕະໂນມັດ ເຊັ່ນວ່າ:

Administrator

- ກວດສອບການເຮັດສໍາລະກົນໃຊ້ໂພດ

ໄພຄຸກຄາມຄອມພິວເຕີ ແລະ ວິທີຈັດການ(Host Threats and Countermeasures)



- Denial of service

- Denial of service ເປັນການໂຈມຕີທີ່ເຮັດໄດ້ຫຼາຍວິທີອີງຕາມໂຄງສ້າງຂອງລະບົບ, ສໍາລັບເຄື່ອງຄອມພິວເຕີ ຜູ້ບຸກໂຈມຕີສາມາດລົບກວນບໍລິການຕ່າງໆຂອງໂປຣແກຣມນໍາໃຊ້ ເຊັ່ນວ່າ: ຜູ້ບຸກໂຈມຕີອາດຈະຮູ້ຈຸດອ່ອນຂອງໂປຣແກຣມຢູ່ໃນລະບົບ ຫຼື ລະບົບປະຕິບັດການ.

- ການປ້ອງກັນ

- ການຕັ້ງຄ່າໂປຣແກຣມ, ບໍລິການ ແລະ ລະບົບປະຕິບັດການບໍ່ໃຫ້ມີຊ່ອງໂວ່ໃນການໂຈມຕີ.
- ປັບປຸງຄວາມປອດໄພລະບົບ ແລະ ຄວາມປອດໄພ Patches
- ປ້ອງກັນການໂຈມຕີ TCP/IP

ໄພຄຸກຄາມຄອມພິວເຕີ ແລະ ວິທີຈັດການ(Host Threats and Countermeasures)



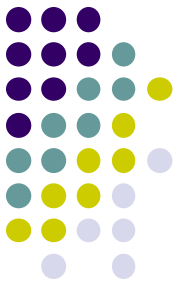
- **Arbitrary code execution**

- ຖ້າຜູ້ບຸກໂຈມຕີສາມາດສັ່ງໃຫ້ຄໍາສັ່ງໂປຣແກຣມເຮັດວຽກໄດ້ຢູ່ໃນເຄື່ອງເຊີເວີໄດ້ຈະເຮັດໃຫ້ສາມາດເຂົ້າເຖິງຂໍ້ມູນຕ່າງໆໄດ້. ສະນັ້ນ, ຈະເຮັດໃຫ້ມີຄວາມສ່ຽງຕໍ່ການສູນເສຍຂໍ້ມູນ.
- ຄວາມສ່ຽງ ແລະ ຊ່ອງໂວ່ທີ່ພາໃຫ້ເກີດຂຶ້ນໄດ້ເຊັ່ນວ່າ: ການຕັ້ງຄ່າເວບເຊີເວີບໍ່ມີຄວາມປອດໄພ ແລະ ບໍ່ມີການປັບປຸງ Patched ຄວາມປອດໄພຂອງເຄື່ອງເຊີເວີ.

- **ການປ້ອງກັນ**

- ຕັ້ງຄ່າເວບເຊີເວີໃຫ້ມີຄວາມປອດໄພ.
- ຈຳກັດຄໍາສັ່ງລະບົບ ແລະ ການເຂົ້າເຖິງຂໍ້ມູນຂອງຜູ້ໃຊ້.
- ປັບປຸງ Patched ຄວາມປອດໄພຂອງເຄື່ອງເຊີເວີ.

ໄພຄຸກຄາມຄອມພິວເຕີ ແລະ ວິທີຈັດການ(Host Threats and Countermeasures)



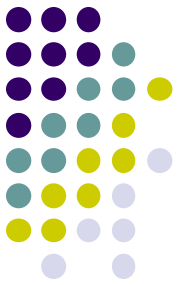
- **Unauthorized access**

- ການຄວບຄຸມການເຂົ້າເຖິງຂໍ້ມູນທີ່ບໍ່ມີການຮັດກຸມຈະເຮັດໃຫ້ຜູ້ໃຊ້ທີ່ບໍ່ໄດ້ຮັບການອະນຸຍາດລ່ວງເຂົ້າໄປຍັງຂໍ້ມູນ ຫຼື ລະບົບທີ່ສໍາຄັນໄດ້.
- ຊ່ອງໂວ່ທີ່ເຮັດຜູ້ໃຊ້ທີ່ບໍ່ໄດ້ຮັບການອະນຸຍາດເຂົ້າເຖິງຂໍ້ມູນໄດ້ມີດັ່ງນີ້:
 - ການຕັ້ງຄ່າເວບເຊີເວີ ແລະ ບັນຊີຜູ້ໃຊ້ FTP server ບໍ່ຮັດກຸມ.
 - ສິດທິຂອງລະບົບໄຟລ NTFS ມີຈຸດອ່ອນ.

- **ການປ້ອງກັນ**

- ຕັ້ງຄ່າເວບເຊີເວີໃຫ້ມີຄວາມໃຫ້ຜູ້ໃຊ້ເຂົ້າເຖິງຂໍ້ມູນຢ່າງປອດໄພ.
- ກຳນົດສິດທິໃຫ້ກັບໄຟລ ແລະ ໄດແຮັກທໍຣີ ດ້ວຍສິດທິແບບ NTFS ໄຟລ.

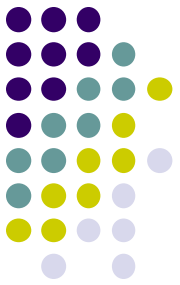
ໄພຄຸກຄາມທາງໂປຣແກຣມ ແລະ ວິທີຈັດການ (Application Threats and Countermeasures)



▪ ວິທີການວິເຄາະໄພຄຸກຄາມທີ່ດີລະດັບໂປຣແກຣມຈະມີການຈັດເປັນໝວດຂອງຊ່ອງໂວ່ຂອງໂປຣແກຣມດັ່ງລຸ່ມນີ້:

- Input validation
- Authentication
- Authorization
- Configuration management
- Sensitive data
- Session management
- Cryptography
- Parameter manipulation
- Exception management
- Auditing and logging

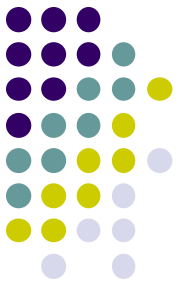
ໄພຄຸກຄາມທາງໂປຣແກຣມ ແລະ ວິທີຈັດການ (Application Threats and Countermeasures)



■ Input validation

- ການປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້ຜ່ານໜ້າໂປຣແກຣມກໍ່ເປັນບັນຫາຄວາມປອດໄພອັນໜຶ່ງຖ້າຜູ້ບຸກໂຈມຕີຄົ້ນພົບວ່າບໍ່ມີຄວາມປອດໄພ ເຊັ່ນວ່າ: ບໍ່ມີການກຳນົດຊະນິດຂໍ້ມູນ, ຄວາມຍາວ, ຮູບແບບ ແລະ ຊ່ວງຂອງຂໍ້ມູນທີ່ຈະປ້ອນ.
- ຊ່ວງໄວ້ຂອງການປ້ອນຂໍ້ມູນມີດັ່ງນີ້:
- Buffer overflows
- Cross-site scripting
- SQL injection
- Canonicalization

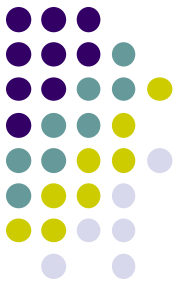
ໄພຄຸກຄາມທາງໂປຣແກຣມ (Application Threats)



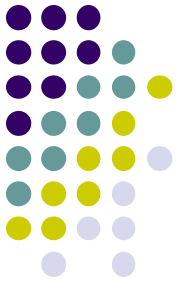
■ Authentication

- ການຢືນຢັນຜູ້ໃຊ້ເປັນວິທີການໃນການປ້ອງກັນການບຸກໂຈມຕີຜ່ານທາງໂປຣແກຣມ, ຊຶ່ງມີຫຼາຍວິທີໃນການນຳໃຊ້ຂຶ້ນກັບຄວາມຕ້ອງການຂອງລະບົບ. ຖ້າບໍ່ມີການຢືນຢັນຜູ້ໃຊ້ຈະເຮັດໃຫ້ໂປຣແກຣມມີຊ່ອງໂວ່ ເຊັ່ນວ່າ:
 - **Network eavesdropping**
 - **Brute force attacks**
 - **Dictionary attacks**
 - **Cookie replay attacks**
 - **Credential theft**

ຂໍ້ມູນອ້າງອີງ



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



ព្យាបាល និង ព័ត៌មាន

ឧបករណ៍