MIS 5170

Operating System Security

Week 14

Unix/Linux

Network Controls

Fox School of Business
TEMPLE UNIVERSITY®

Tonight’s Plan

- ❑ Questions from Last Week
- ❑ Review on-line posts
- ❑ In The News
- ❑ Network Controls
- ❑ Review for Test 2
- ❑ Assignment 4
- ❑ Next Week
- ❑ Quiz

Questions From Last Week

- Any Questions from last week?
- Review of quiz questions
  - What are Unix/Linux start-up modes? Run Levels? Init Levels? (40%)
    - /etc/rc*.d
    - service --status-all
  - How would you uninstall a package? (42%)
    - Remember installing and removing packages uses apt-get
  - Kali CIS baseline
    - Know the half a dozen commands used to apply a baseline to Kali

Questions From Last Week (cont)

- Any additional questions?

Review on-line posts

- Review of on-line posts
  - One post from Shain
    - Possible hack from US causing the failure of the test launch
      - https://www.thesun.co.uk/news/3342396/north-korea-missile-launch-failure-us-cyber-attack-sabotage/
  - One post from Mauchel
    - Windows users might want to turn off their computers this weekend
      - http://www.businessinsider.com/hackers-release-nsas-secret-hacking-tools-for-windows-2017-4

Review on-line posts (Cont)

- Questions?

In the News

- Why I Always Tug on the ATM, sounds like a trend, but maybe the owners running these should take this to heart
  - Two more companies credit card system's breached
    - https://krebsonsecurity.com/2017/04/intercontinental-hotel-chain-breach-expands/
    - https://krebsonsecurity.com/2017/04/shoneys-hit-by-apparent-credit-card-breach/
- Use of Secure VPN to use the internet
  - Protect you browsing from your ISP
    - http://thehackernews.com/2017/03/secure-vpn-services.html
- Major leak suggests NSA was deep in the middle east banking system
  - Who needs Area 51 anymore just search the internet…
    - https://www.wired.com/2017/04/major-leak-suggests-nsa-deep-middle-east-banking-system/

In the News (Cont)

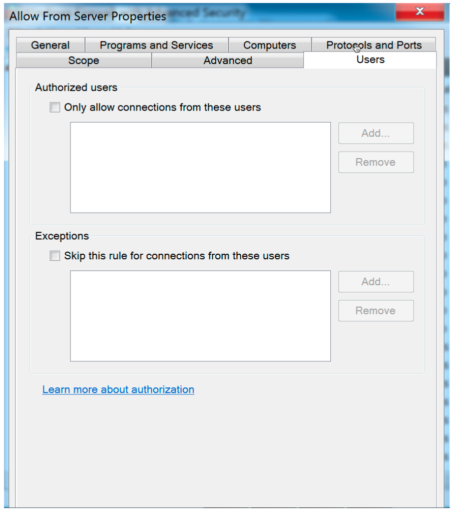
- Questions?

Network Controls

- What is network controls?
- How do we use them?
- How do we configure them?
- How is this different from Windows networking controls?

Network Controls (cont)

- What is network controls?
  - A method of defining what computers are allowed to talk to services on our Unix/Linux system
  - This is similar to what we saw on Windows with the Network Controls, but Users and/or Computers allows or exceptions



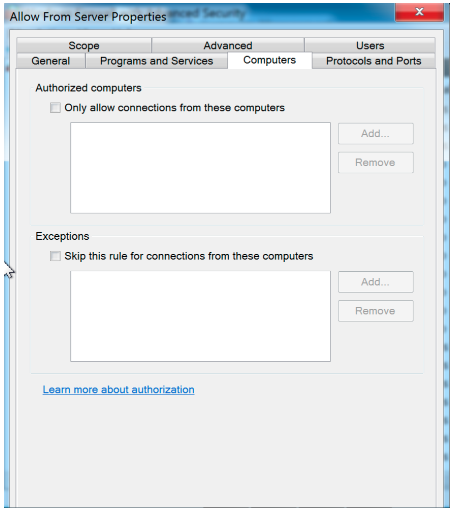
Authorized users

□ Only allow connections from these users

Exceptions

□ Skip this rule for connections from these users

Learn more about authorization



Authorized computers

□ Only allow connections from these computers

Exceptions

□ Skip this rule for connections from these computers

Learn more about authorization

Network Controls (cont)

- How do we use them?
  - Manage the .deny and the .allow file
  - Create rules that list where (ip address) services can connect to our operating system
  - In conjunction with FireWall rules
  - Review the man pages
    - man hosts.allow
    - man hosts.deny
  - Example:
    - /etc/hosts.deny
      - finger : ALL : DENY

Network Controls (cont)

- How do we configure them?
  - Modify the following for deny
    - /etc/hosts.deny
  - Modify the following for allow
    - /etc/hosts.allow

Network Controls (cont)

- How is this different from Windows networking controls?
  - These settings are part of the networking layer where as on Windows it is part of the FireWall layer
- Prevent Root from using SSH
  - Modify /etc/ssh/sshd_config
    - Change the line PermitRootLogin
- Demo

Review for Test 2

- Review Quiz 5
- Review Quiz 6
- Review Quiz 7

Review for Test 2 (Quiz 5)

- Any Questions from last week?
  - Windows FireWall Logging
    - How do we enable it?
      - Server Manager
  - Windows FireWall configuration that protects protocols
    - Telent would an insecure protocol
      - IPSec is the configuration that protects insecure protocols
        - How do you turn this on?
          - These are listed under “Windows Security Rules”
  - What is as important as enabling logging?

Review for Test 2 (Quiz 6)

- Any Questions from last week?
- Review of quiz questions
  - How do you create a Unix/Linux script?
    - Remember you need to create it and use chmod to set the execution bit
  - SHA 1 has been cracked
    - Why is sha256
      - CRC is used for communication verification not mathematical summations
  - How do you get the members of a group
    - Right: getent group <Group Name>
    - Wrong: cat /etc/group

Review for Test 2 (Quiz 7)

- Any Questions from last week?
- Review of quiz questions
  - What are Unix/Linux start-up modes? Run Levels? Init Levels? (40%)
    - /etc/rc*.d
    - service --status-all
  - How would you uninstall a package? (42%)
    - Remember installing and removing packages uses apt-get
  - Kali CIS baseline
    - Know the half a dozen commands used to apply a baseline to Kali

Assignment 4 Review

- ❑ Shared VM's with the Wade's class
- ❑ Will get the results
- ❑ Will post the grades; may have a field trip or Saturday class to talk about the findings and/or corrections

Next Week

- Test 2 will be based on this week’s Network Controls and slides from the second half of the class.
- Review of Assignment 4 findings
- Test 2

Quiz

- We can start the Quiz