

MIS 5170

Operating System Security

Week 14

Unix/Linux Network Controls

Tonight's Plan

2

- ❑ 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

3

- ❑ Any Questions from last week?
- ❑ Review of quiz questions
 - ❑ How to you enable logging on Unix/Linux
 - Remember using iptables with (iptables -A INPUT -j LOGGING)
 - ❑ How do you watch the firewall log on Unix/Linux
 - Tail the messages file under logs
 - ❑ Kali CIS baseline
 - Know the half a dozen commands used to apply a baseline to Kali

Questions From Last Week (cont)

4

- Any additional questions?

Review on-line posts

5

- Review of on-line posts
 - ▣ One post from Sev
 - IOT Hack
 - https://www.dailydot.com/debug/casino-hack-fish-tank/?utm_content=casino-hack-fish-tank&utm_medium=syndication&utm_source=LinkedIn&utm_name=linkedin-syndication
 - ▣ One post from Fred
 - Scans for home routers (Change router defaults)
 - <https://www.us-cert.gov/ncas/alerts/TA18-106A>

Review on-line posts (Cont)

6

- Questions?

In the News

7

- ❑ When Identity Thieves Hack Your Accountant
 - ❑ The Internal Revenue Service has been urging tax preparation firms
 - <https://krebsonsecurity.com/2018/04/when-identity-thieves-hack-your-accountant/>
- ❑ Use of Secure VPN to use the internet
 - ❑ Protect you browsing from your ISP
 - <http://thehackernews.com/2017/03/secure-vpn-services.html>
- ❑ 'iTunes Wi-Fi Sync' Feature Could Let Attackers Hijack Your iPhone, iPad Remotely
 - ❑ Why you should always carry your...
 - <https://thehackernews.com/2018/04/iphone-itunes-wifi-sync.html>



In the News (Cont)

8

- Questions?

Network Controls

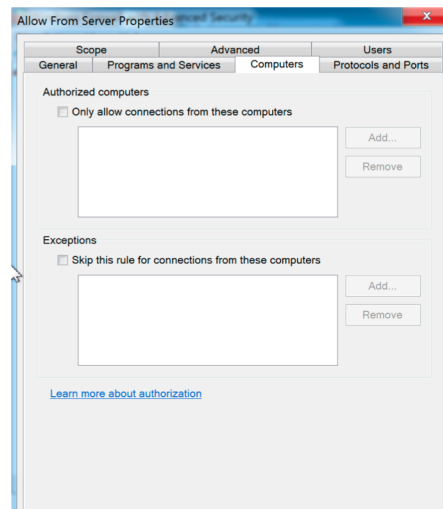
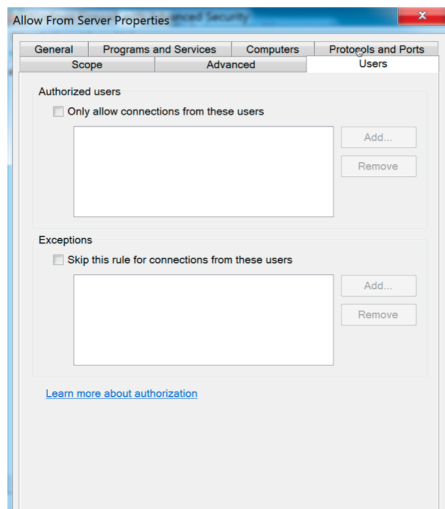
9

- ❑ 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)

10

- ❑ 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



Network Controls (cont)

11

- 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)

12

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

Network Controls (cont)

13

- ❑ 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

14

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

Review for Test 2 (Quiz 5)

15

- Any Questions from last week?
 - Windows FireWall Logging
 - How do we enable it?
 - Server Manager
 - Windows FireWall configuration that protects protocols
 - Telnet 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)

16

- ❑ 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)

17

- ❑ 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

18

- ❑ 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

19

- ❑ 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

20

- ❑ We can start the Quiz