MIS 5170

Operating System Security

Week 11

Unix/Linux

Configuration Management

Fox School of Business
TEMPLE UNIVERSITY®

Tonight's Plan

- Questions from Last Week
- Review on-line posts
- In The News
- Configuration management practices
- Unix/Linux System hardening
- Baselines
- Assignment 4 Overview
- Next Week
- Quiz

Questions From Last Week (Quiz 5)

- Any Questions from last week?
  - Switched networks and sniffers
    - What is one technique you need to use in a switched network?
      - Software sniffers
  - What is network analysis software?
    - Also known as network sniffer, netmon, network trace
  - What is as important as enabling logging?

Questions From Last Week (Quiz 6)

- How is logging enabled?
  - Server Manager
    - Open the properties for the firewall
  - 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?

Questions From Last Week (cont)

- Any additional questions?

Review on-line posts

- On-line post:
  - **Fred Zajac:** Monitoring what matters – Windows Event Forwarding for everyone (even if you already have a SIEM.)
    - https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/
  - **Vince Kelly:** How Cisco's newest security tool can detect malware in encrypted traffic
    - https://www.networkworld.com/article/3246195/lan-wan/how-cisco-s-newest-security-tool-can-detect-malware-in-encrypted-traffic.html
- **Fraser G:** Monero-Mining HiddenMiner Android Malware Can Potentially Cause Device Failure
  - https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-hiddenminer-android-malware-can-potentially-cause-device-failure/

Review on-line posts (Cont)

- Questions?

In the News

- Unix/Linux
  - How many devices in your enterprise are running it?
    - Dr. Eric Cole URL is On-Line
      - https://www.beyondtrust.com/resources/webinar/top-3-linux-security-vulnerabilities-fix/?access_code=bb72ff86dcbb43a491a760184828aa78&mkt_tok=eyJpIjoiTlRWbFpHVTRNekEzTTJWbCIsInQiOiJFdDlITENkTFg5SDV0bXJcL0tXRFoxZWt6QVN2TzFqeHhRamRXUG53ZmdcL3ZXQ0VZK0NJcTJnemtjdUhIU3prOFpnaEZyMVFCQjZXUjl1V1JwMHlxQmlCc0tOZTlSVU1hZTFrTlcxVG1keWYzSXBWMk1kQ21OWmlua0x5T05jR2ZwIn0%3D
- **Omitting the "o" in .com Could Be Costly**
  - Why companies buy miss-spelling of their company's URL
    - https://krebsonsecurity.com/2018/03/omitting-the-o-in-com-could-be-costly/
- **Atlanta Ransome-ware…**
  - Time Is Running Out For Atlanta In Ransomware Attack
    - Lots of sites

In the News (Cont)

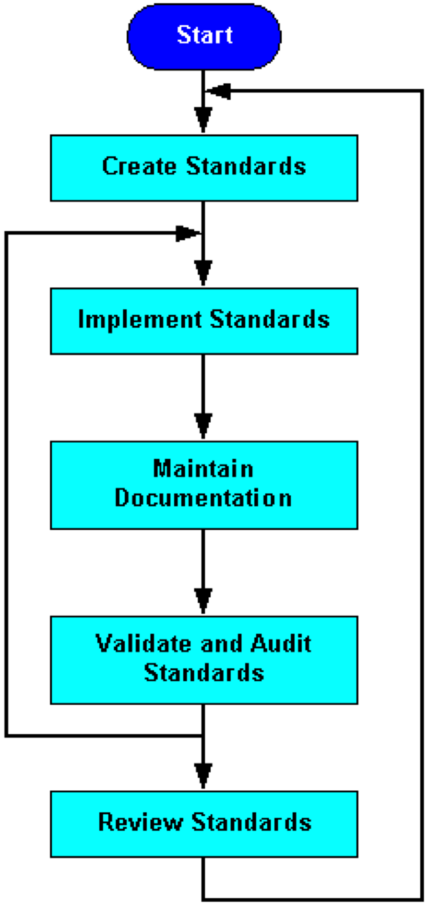
- Google Chrome to Distrust Symantec SSLs for Mis-issuing 30,000 EV Certificates
  - EV Cert Trust Wars ("my words")
    - http://thehackernews.com/2017/03/google-invalidate-symantec-certs.html
- Questions?

Configuration Management Practices

- Remember these from Week 4?
  - We looked at these on Windows; now on Unix/Linux
- What is configuration Management?
- How can it help us?
- How can it secure an operating system?
- What are the steps?

Configuration Management Practices (cont)

- What is configuration Management?
  - Configuration Management is a set of steps that creates and maintains consistency in our case of an operating system.
  - This can be rigorous as a Baseline, which we will look at later tonight.
  - Can be as simple as a run-book, which is a set of documents that is followed when installing an operating system or application on top of said operating system.

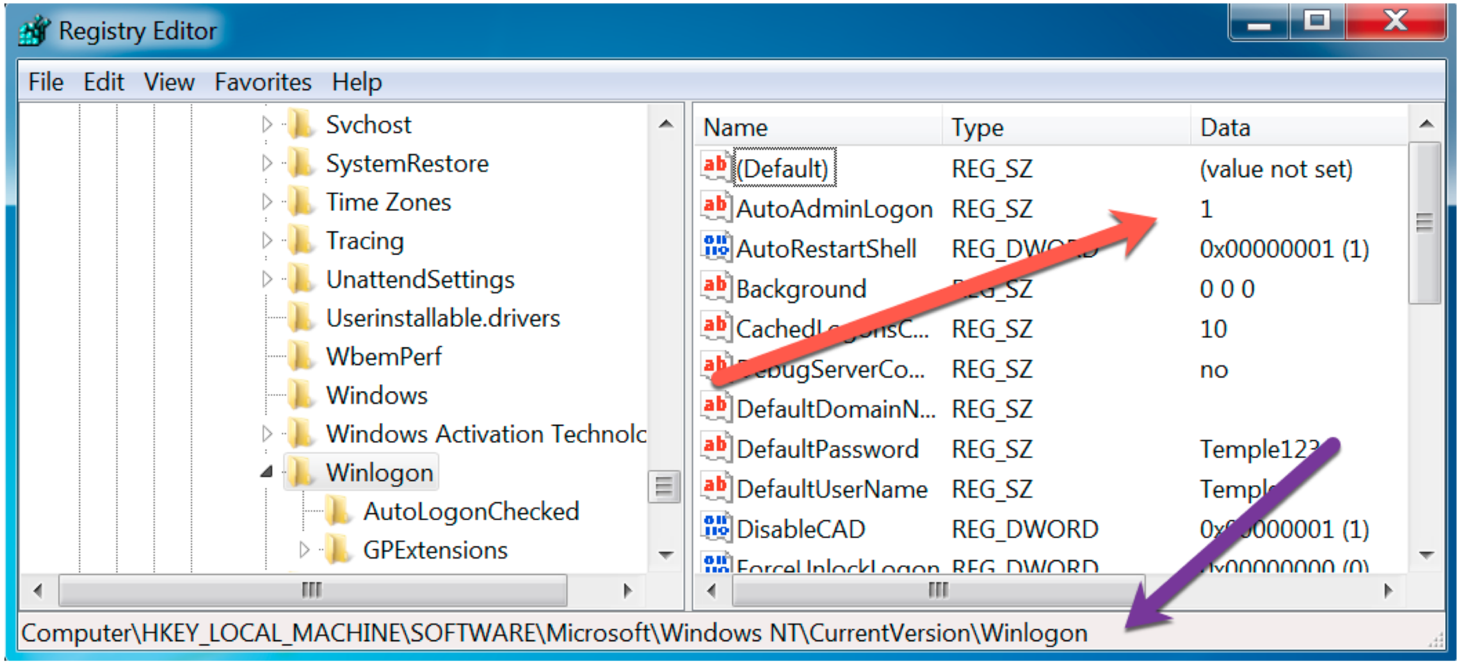


Configuration Management Practices (cont)

- How can it help us?
  - This can help us to find deviation when we run a baseline difference scan.
    - Baseline Difference Scan = what has changed or is no longer equal to a setting we want to maintain
  - Tools like PowerShell Desired State Configuration on Windows
  - With Unix/Linux tools like puttet
    - Learn Puppet is the following link:
      - https://puppet.com/download-learning-vm?ls=paid-search&ccn=digital-PMG-pe&pub=bing&cid=701G0000001dTYu&utm_medium=paid-search&utm_campaign=digital-PMG-pe&utm_source=bing&utm_content=learning-vm&utm_term=puppet

Configuration Management Practices (cont)

- How can it secure an operating system?
  - Track things we don't want to ever see; and flag them as invalid values in areas we have seen last week.

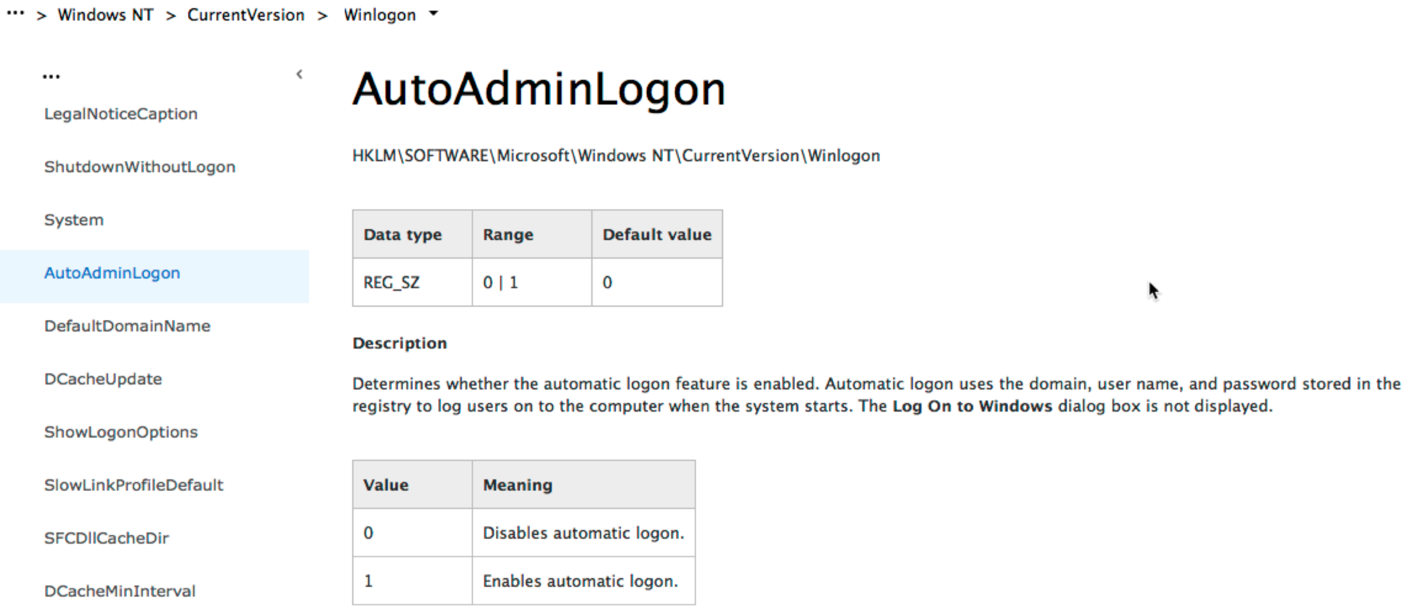


Name	Type	Data
(Default)	REG_SZ	(value not set)
AutoAdminLogon	REG_SZ	1
AutoRestartShell	REG_DWORD	0x00000001 (1)
Background	REG_SZ	0 0 0
CachedLogonsC...	REG_SZ	10
DebugServerCo...	REG_SZ	no
DefaultDomainN...	REG_SZ	
DefaultPassword	REG_SZ	Temple123
DefaultUserName	REG_SZ	Temple
DisableCAD	REG_DWORD	0x00000001 (1)
ForceUnlockLogon	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Configuration Management Practices (cont)

- How can it secure an operating system? (cont)
  - By tracking and alerting for those settings that just should not be in the environment.
    - https://technet.microsoft.com/en-us/library/cc939702.aspx



AutoAdminLogon

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Data type	Range	Default value
REG_SZ	0 | 1	0

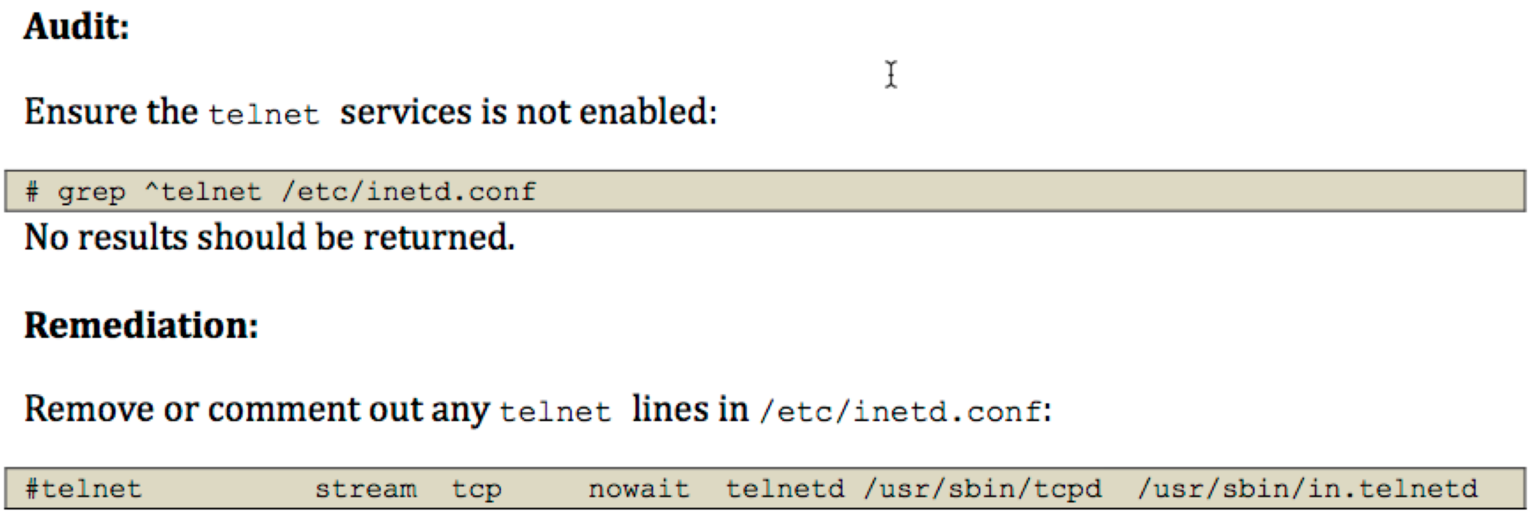
Description

Determines whether the automatic logon feature is enabled. Automatic logon uses the domain, user name, and password stored in the registry to log users on to the computer when the system starts. The **Log On to Windows** dialog box is not displayed.

Value	Meaning
0	Disables automatic logon.
1	Enables automatic logon.

Configuration Management Practices (cont)

- How can it secure an operating system?
  - Telnet



Audit:

Ensure the `telnet` services is not enabled:

```
# grep ^telnet /etc/inetd.conf
```

No results should be returned.

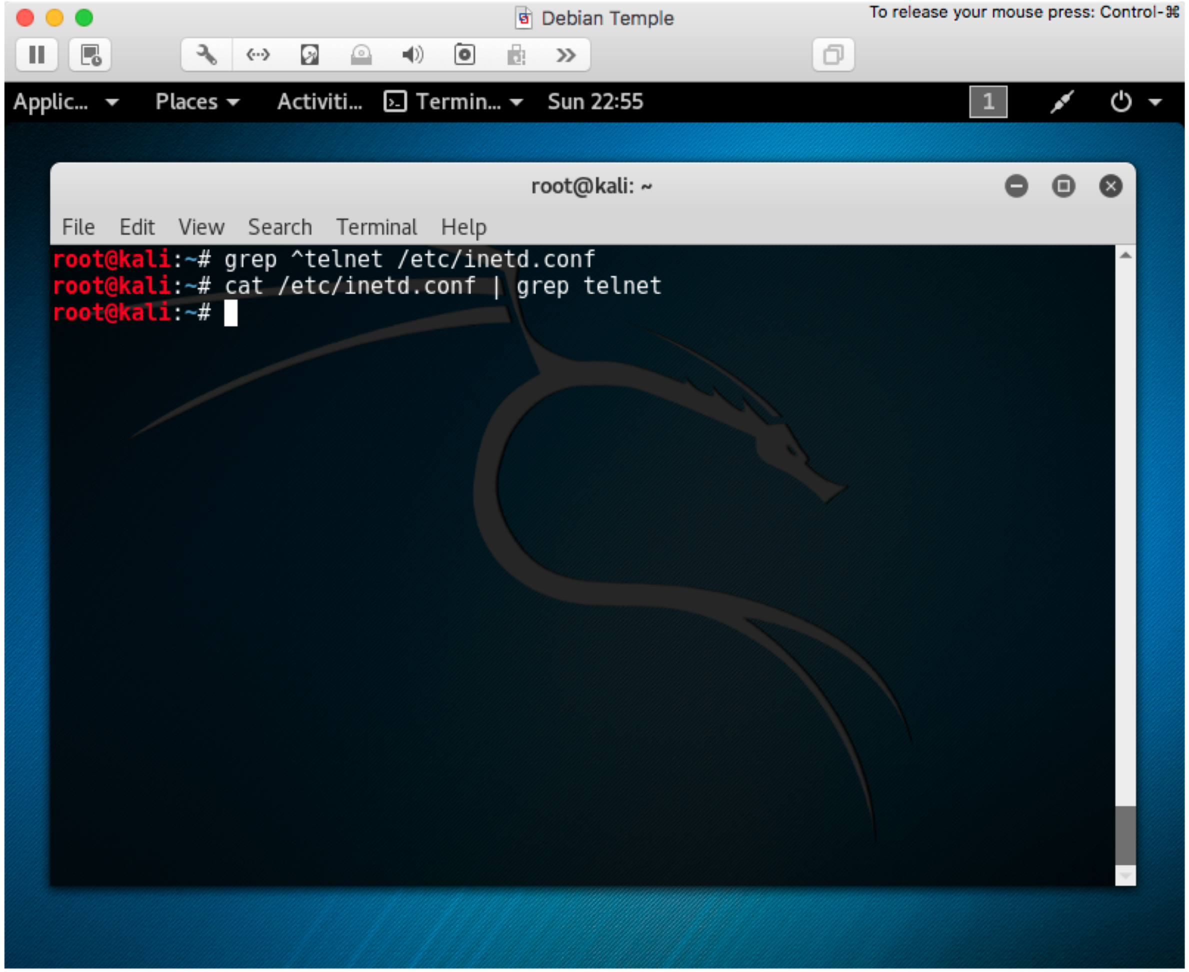
Remediation:

Remove or comment out any `telnet` lines in `/etc/inetd.conf`:

```
#telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
```

Configuration Management Practices (cont)

- Telnet



Debian Temple
To release your mouse press: Control-⌘
Applic... Places Activiti... Termin... Sun 22:55
root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# grep ^telnet /etc/inetd.conf
root@kali:~# cat /etc/inetd.conf | grep telnet
root@kali:~# 
```

Configuration Management Practices (cont)

- What are the steps?
  - Review company policies or best practices like:
    - CIS Debian Baseline: On-Line
  - Create a run-book or use tools like puppet
  - Create a script or an Image, similar to what we have done with our snap-shots
  - Run a difference baseline to see if there is drift
    - If so chose set them back or alert on drift

Configuration Management Practices (cont)

- Questions?

Unix/Linux System hardening

- What is system hardening?
- How do you know what to turn off?
- Using a baseline to help

Unix/Linux System hardening (cont)

- What is system hardening?
  - System hardening is to remove default services or configuration from running or being part of the operating system.
    - Removing or shutting down services
    - Changing the default setting(s) to what your enterprise needs or company policy and/or standards says

Unix/Linux System hardening (cont)

- How do you know what to turn off?
  - Anything that is not needed to make your operating system function as needed for the use case.
    - Example:
      - Default AWS AMI
        - Turn off all services except inbound ssh
          - Update-rc.d ssh enable

Unix/Linux System hardening (cont)

- Using a baseline to help
  - Review what it is doing
  - Apply those that keeps from breaking your operating system for it’s primary usage
    - Example: if you need it to print; don’t turn off cups or lpr/lpd services

Unix/Linux System hardening (cont)

- Questions?

Baselines

- What is a Baseline?
- How can this help us?
- What are some Baselines?
- Specific Details about Baselines.
- Demo

Baselines (cont)

- What is a Baseline?
  - A Baseline is (aka Merriam-Webster) – information that is used as a starting point by which to compare other information.
    - Not very helpful?
    - For a computer the starting point is when you install it from an ISO.
  - Let us think of it as What we want a computer to allow it's users or process to be able to do or not do. A minimum security model, 'Least Privileges' or where is that line in the sand?

Baselines (cont)

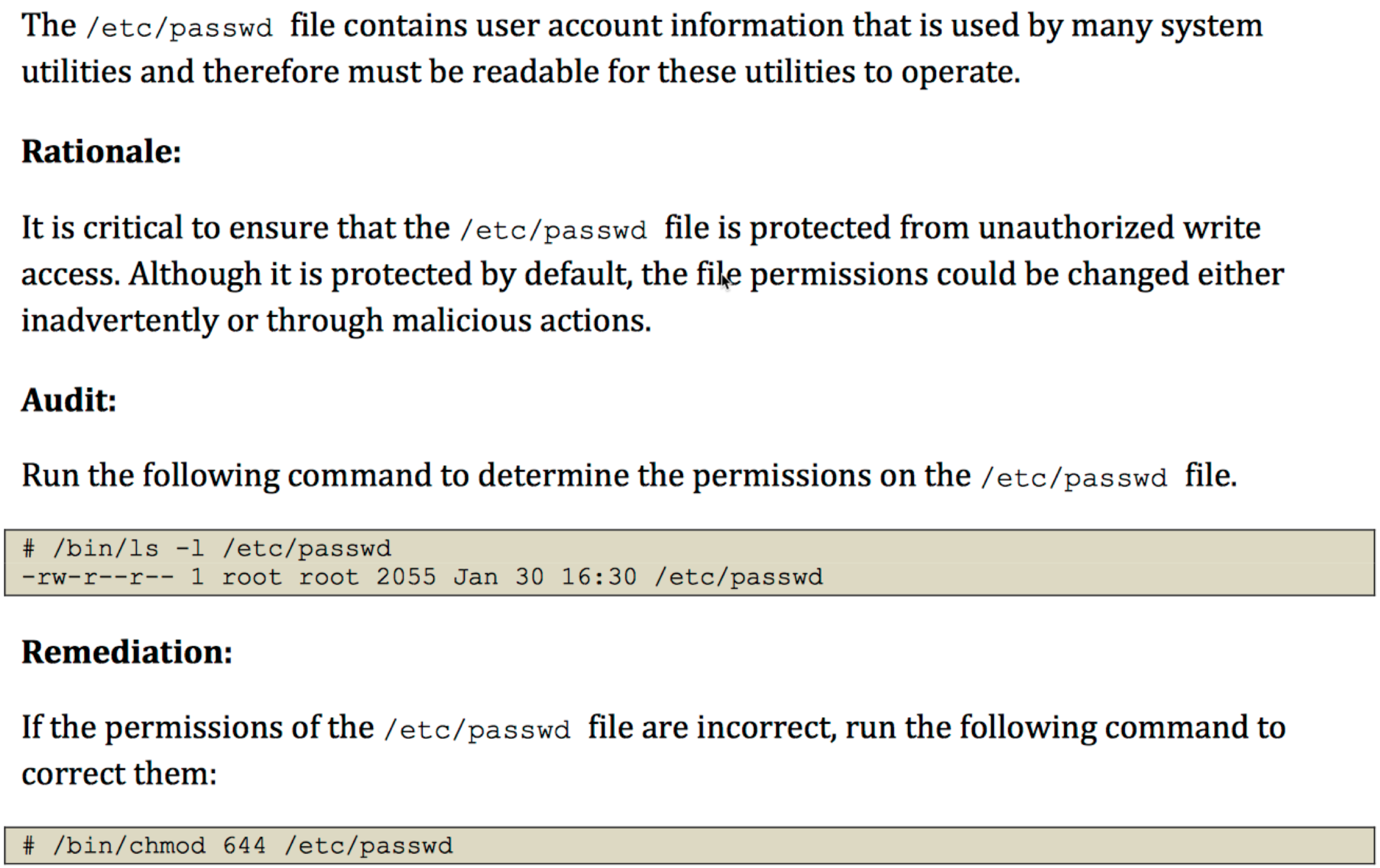
- How can this help us?
  - This can help us trigger that something is wrong or someone is trying to make something go wrong.
  - Should we write a vulnerability (Possibly known as a ‘Risk’) against the delta or is it an exception we should track
  - Should we tighten up from detective to preventative?
- These are some questions that could help frame the specifics of what we find.

Baselines (cont)

- What are some Baselines?
  - NIST – National Institute of Standards and Technology
    - https://usgcb.nist.gov/usgcb/rhel/download_rhel5.html
  - CIS Benchmark – Center for Internet Security.
    - http://community.mis.temple.edu/mis5170sec001sp2017/files/2015/12/CIS_Debian_Linux_7_Benchmark_v1.0.0.pdf
  - ISO 27002 – Information security standard published by the International Organization for Standardization.
  - ISF – Information Security Forum.
    - https://www.securityforum.org/consultancy/information-security-readiness-benchmark/
  - DISA Baselines
    - http://iase.disa.mil/stigs/os/unix-linux/Pages/index.aspx

Baselines (cont)

- Specific Details about Baselines.



The /etc/passwd file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.

Rationale:

It is critical to ensure that the /etc/passwd file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command to determine the permissions on the /etc/passwd file.

```
# /bin/ls -l /etc/passwd
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/passwd
```

Remediation:

If the permissions of the /etc/passwd file are incorrect, run the following command to correct them:

```
# /bin/chmod 644 /etc/passwd
```

Baselines (cont)

- Demo

Baselines (cont)

- Questions?

Assignment 4 Overview

- Requirements – Same teams members as before
- Prep your VM
- Share with Wade’s class
- Get outside assessment of how you did

Next Week

- Assignment 4 Due Friday April 7th 11:59 pm

Quiz

- We can start the Quiz