Security in the Real World: **Compliance**

Reese Pearsall
CSCI 476 Spring 2021

Reese Pearsall (pierce-all)

Current Graduate Student @MSU
B.S. Computer Science @ MSU

Interests
- Cybersecurity
- Cyber crime
- Malware Analysis

Teaching
- CSCI 127
- CSCI 460 (TA)

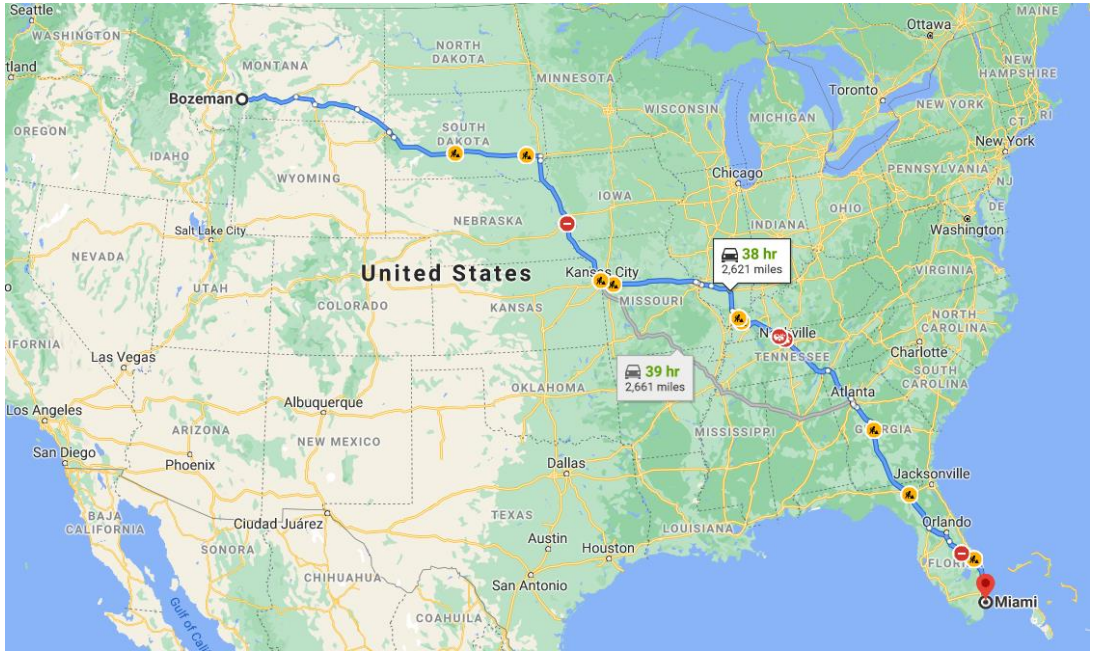
Experience
- TechLink -> Bozeman, MT (Software Engineering & Testing)
- United States Air Force -> Ogden, UT (Software Engineering)
- **(Current)** Hoplite Industries -> Bozeman, MT (Software Engineering)

Outside of Academia…
- Video games, New England Patriots, Fantasy Football, Movies, Dogs, Memes, Discord, *The Bachelor*

website: reesep.github.io

Activity- Preparing for a Road trip

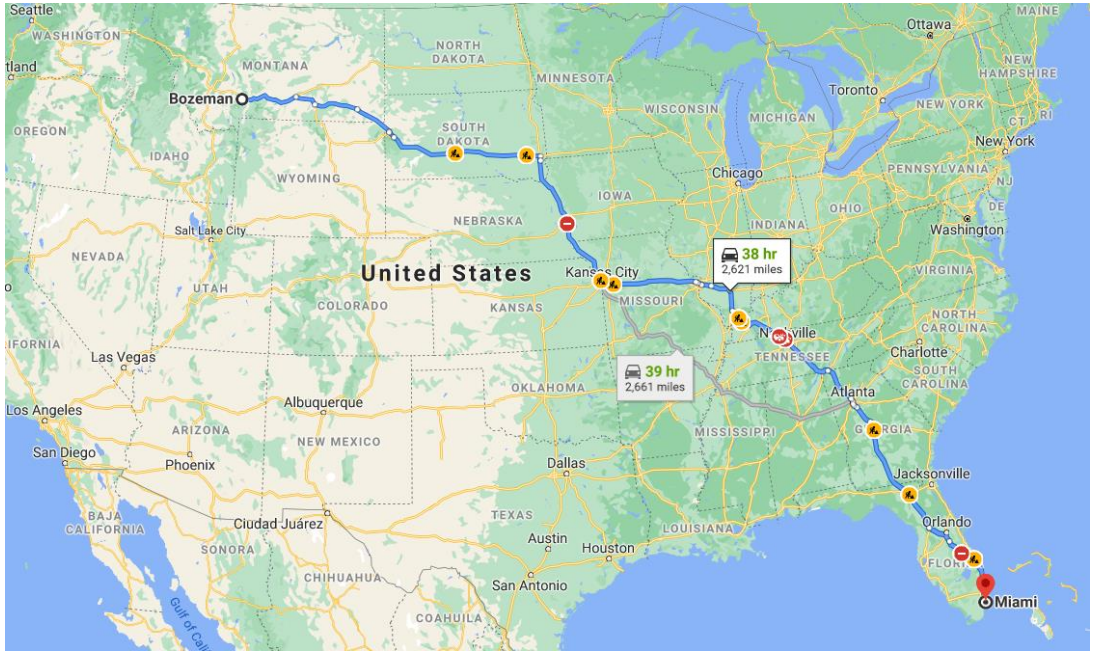
Suppose you and your friends are planning a road trip to Miami this summer



Activity- Preparing for a Road trip

Suppose you and your friends are planning a road trip to Miami this summer

You just purchased a used car that you have never driven before and don’t know very much about

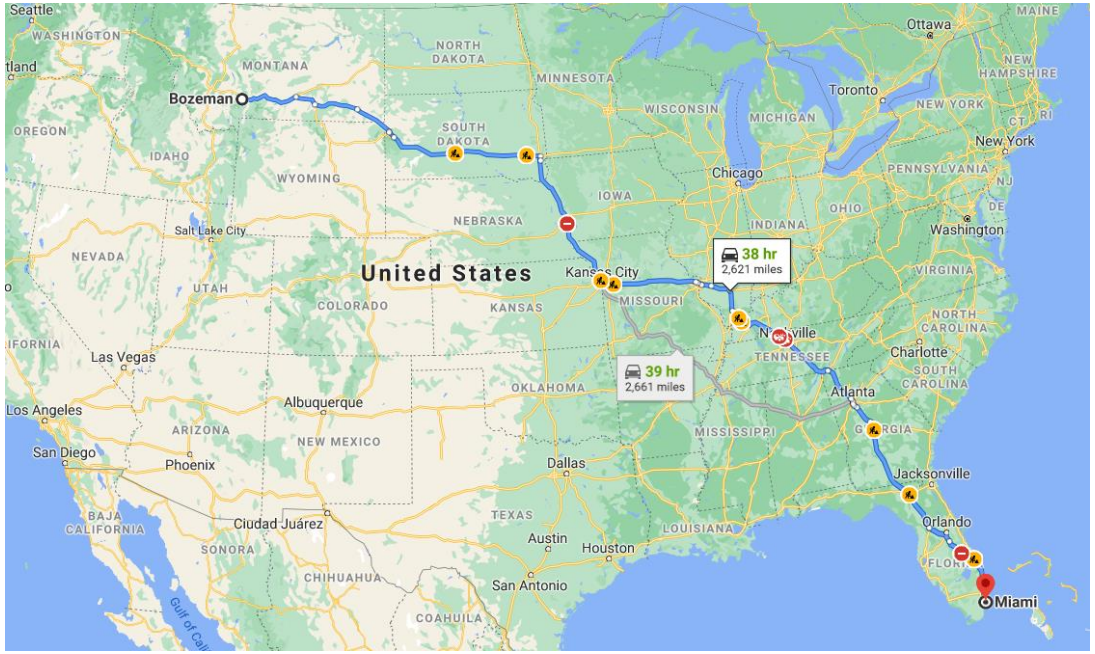


Activity- Preparing for a Road trip

Suppose you and your friends are planning a road trip to Miami this summer

You just purchased a used car that you have never driven before and don’t know very much about

Before you go on the road trip, what kind of inspections or checks should you conduct to ensure nothing goes wrong while traveling?



Activity- Preparing for a Road trip

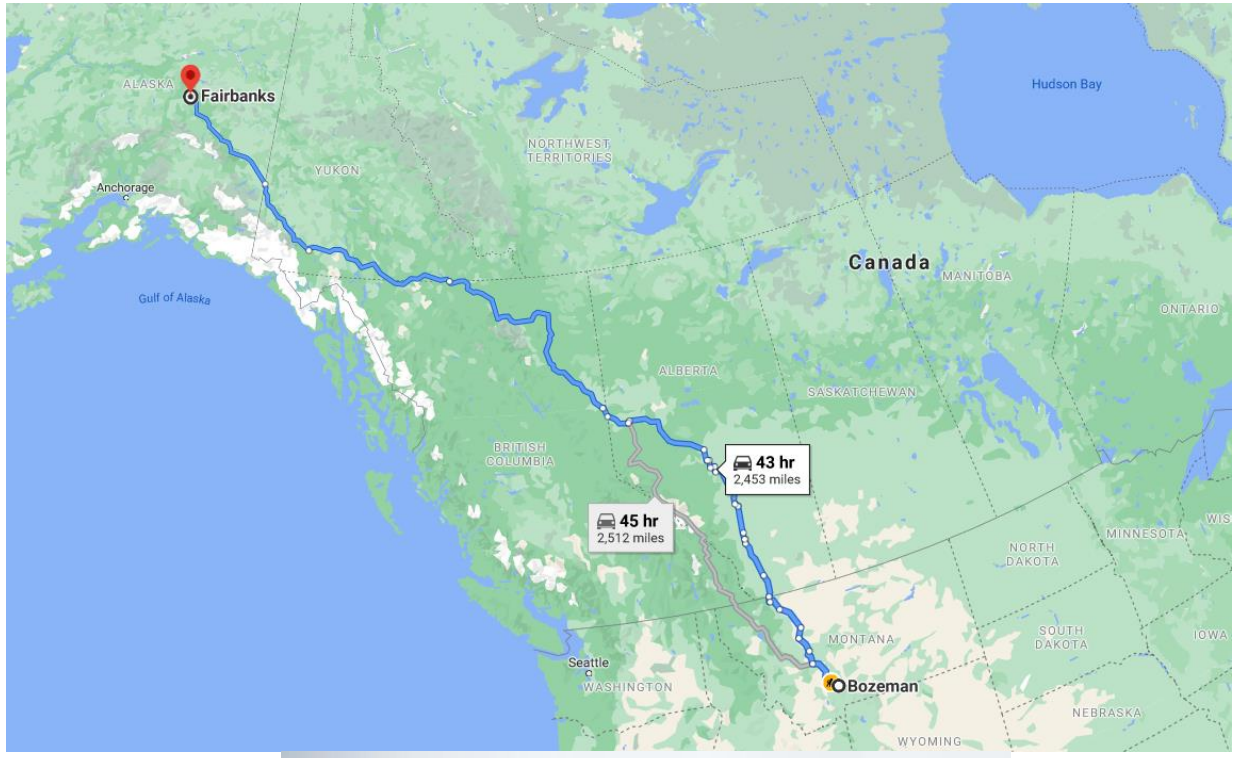
Suppose you and your friends are planning a road trip to Miami this summer

You just purchased a used car that you have never driven before and don’t know very much about

Before you go on the road trip, what kind of inspections or checks should you conduct to ensure nothing goes wrong while traveling?

Activity- Preparing for a Road trip (Winter)

Suppose the trip to Miami didn't happen

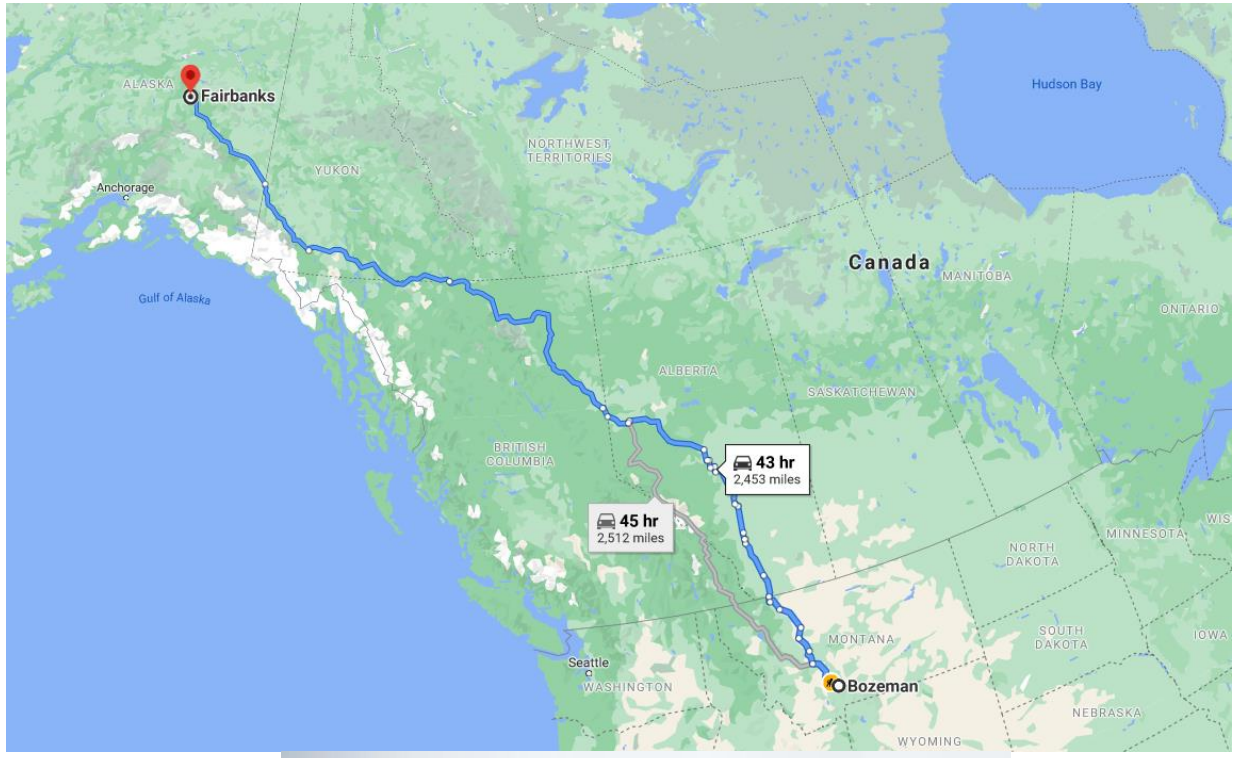


Activity- Preparing for a Road trip (Winter)

Suppose the trip to Miami didn't happen

Now, you and your friends and planning a trip to Fairbanks, Alaska in January

Is your checklist going to be the same? What would be different?



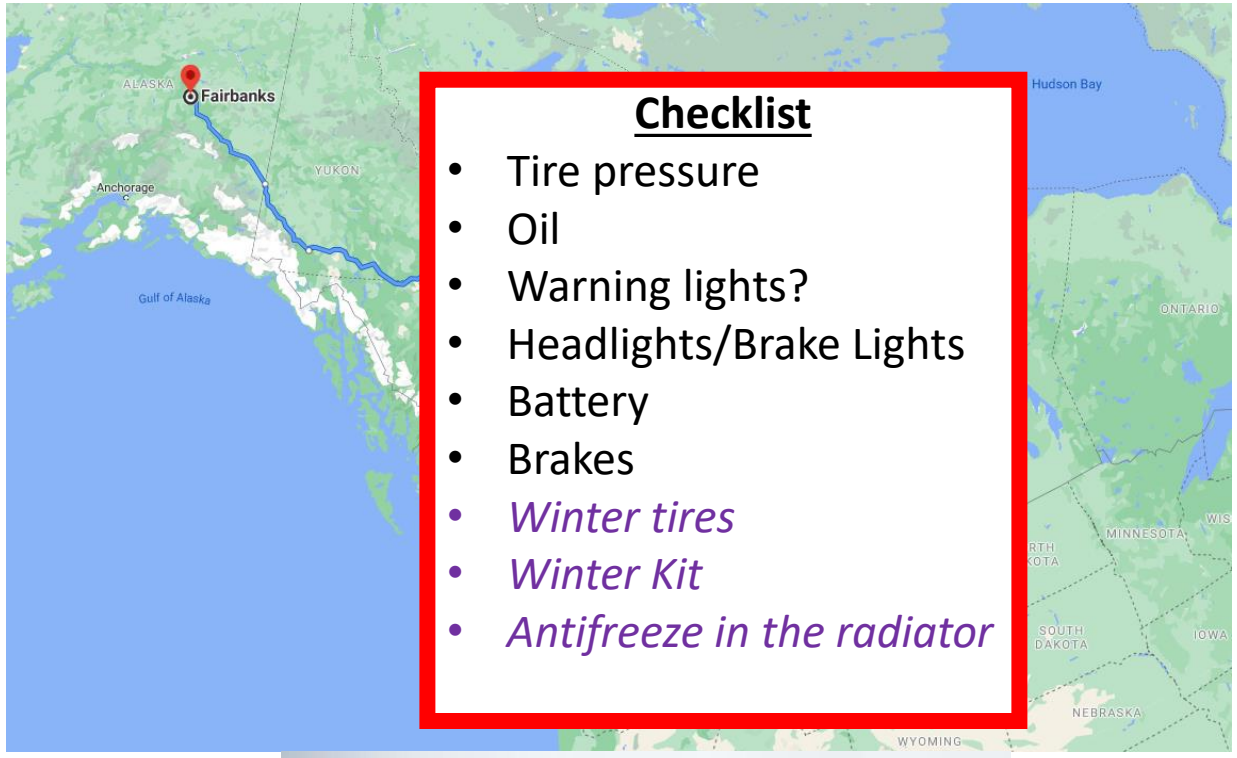
Activity- Preparing for a Road trip (Winter)

Suppose the trip to Miami didn't happen

Now, you and your friends and planning a trip to Fairbanks, Alaska in January

Is your checklist going to be the same? What would be different?

It will look similar, but there will probably be a few more additional things to check!



Checklist

- Tire pressure
- Oil
- Warning lights?
- Headlights/Brake Lights
- Battery
- Brakes
- *Winter tires*
- *Winter Kit*
- *Antifreeze in the radiator*

Activity- Securing an environment

Let’s move to a more relevant example….

Suppose you were hired as the new system administrator at a local tech company

Activity- Securing an environment

Let’s move to a more relevant example….

Suppose you were hired as the new system administrator at a local tech company

Your boss asks you to evaluate the company work server, which is running a version of Ubuntu. Your boss wants to make sure there are no possible vulnerabilities with the current system

Activity- Securing an environment

Let’s move to a more relevant example….

Suppose you were hired as the new system administrator at a local tech company

Your boss asks you to evaluate the company work server, which is running a version of Ubuntu. Your boss wants to make sure there are no possible vulnerabilities with the current system

What sorts of things would you check on the system?
Think about some of things you learned this semester…

Activity- Securing an environment

Does anything change?

Activity- Securing an environment

Does anything change?

Yes! Adding a SQL server to the stack adds new potential vulnerabilities (SQL Injections, Data Leaks, etc)

What is compliance?

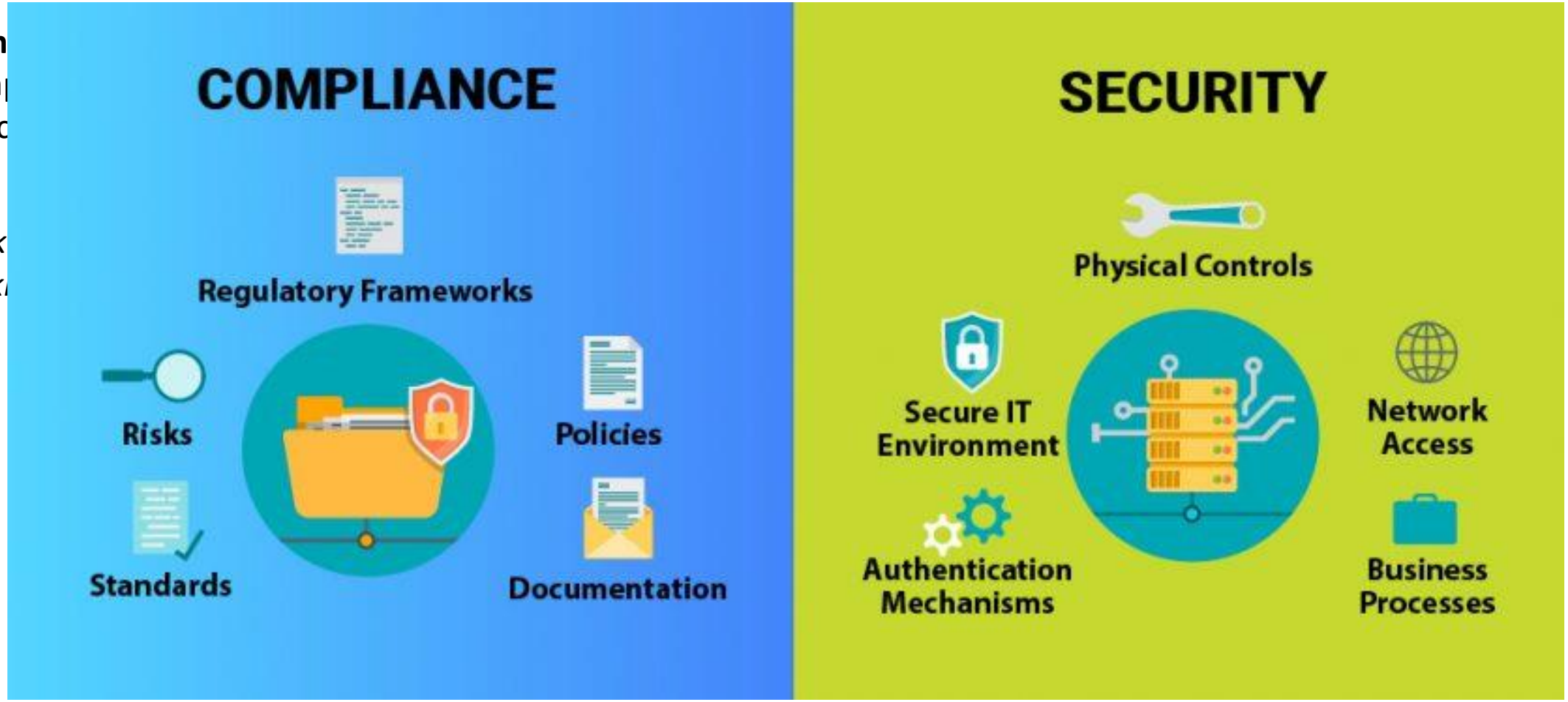
Compliance – ensuring that rules/policies are being followed and companies are meeting security-related requirements. These rules are typically set my government, industry, or other 3rd parties

"Taking a snapshot of a company's technical infrastructure and making sure it follows some kind of regulatory framework"

What is compliance?

Com
comp
typic

"Tak
maki



What are these “rules”?

These rules are structured as a **compliance framework**, which is a structures set of guidelines and best practices that details a company’s processes for meeting regulatory requirements

What are these “rules”?

These rules are structured as a **compliance framework**, which is a structures set of guidelines and best practices that details a company’s processes for meeting regulatory requirements

There are many different types of compliance frameworks. The framework that a company utilizes varies by what kind of data the company deals with

What are these “rules”?

These rules are structured as a **compliance framework**, which is a structures set of guidelines and best practices that details a company’s processes for meeting regulatory requirements

There are many different types of compliance frameworks. The framework that a company utilizes varies by what kind of data the company deals with

PCI DSS (Payment Card Industry Data Security Standard)
Compliance framework for companies that process, store, or transmit credit card information

What are these “rules”?

These rules are structured as a **compliance framework**, which is a structures set of guidelines and best practices that details a company’s processes for meeting regulatory requirements

There are many different types of compliance frameworks. The framework that a company utilizes varies by what kind of data the company deals with

HIPPA(Health Insurance Portability and Accountability Act)
Compliance framework for companies that process protected health information

What are these “rules”?

These rules are structured as a **compliance framework**, which is a structures set of guidelines and best practices that details a company’s processes for meeting regulatory requirements

There are many different types of compliance frameworks. The framework that a company utilizes varies by what kind of data the company deals with

NIST(National Institute of Standard and Technology)
General framework for security practices for government agencies

STIG Compliance Framework

STIG (Security Technical Implementation Guide) is a compliance framework developed by Defense Information System Agency used for configuration of computer and network systems

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	414
2	Debian Linux	Debian	OS	360
3	Windows Server 2016	Microsoft	OS	357
4	Windows 10	Microsoft	OS	357
5	Windows Server 2019	Microsoft	OS	351
6	Acrobat Reader Dc	Adobe	Application	342
7	Acrobat Dc	Adobe	Application	342
8	Cpanel	Cpanel	Application	321
9	Windows 7	Microsoft	OS	250
10	Windows Server 2008	Microsoft	OS	248

Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2019

https://www.cvedetails.com/top-50-products.php?year=2019

STIG Example

Here's an example of a STIG for Red Hat Linux

STIG - 230503

The Red Hat Enterprise Linux operating system must be configured to disable USB mass storage.

Why would this be a rule?

STIG Example

Here's an example of a STIG for Red Hat Linux

STIG - 230503

The Red Hat Enterprise Linux operating system must be configured to disable USB mass storage.

Why would this be a rule?

USB storage permits easy introduction of unknown devices, which could have malicious intentions

STIG Example

Here's an example of a STIG for Red Hat Linux

STIG - 230503

The Red Hat Enterprise Linux operating system must be configured to disable USB mass storage.

STIG - 230534

*The Red Hat Enterprise Linux operating system must be configured so that the root account must be the **only** account having unrestricted access to the system.*

Why would this be a rule?

STIG Example

Here's an example of a STIG for Red Hat Linux

STIG - 230503

The Red Hat Enterprise Linux operating system must be configured to disable USB mass storage.

STIG - 230534

*The Red Hat Enterprise Linux operating system must be configured so that the root account must be the **only** account having unrestricted access to the system.*

Why would this be a rule?

Permissions are important. Someone who has root permissions could potentially mess up an entire system or could brute force guess a password for a privileged account.

STIG Example

For Red Hat Linux there are 248 different STIGs that need to be checked

There are STIGS for MANY different operating systems and applications

Apache
Apple iOS 12 (42)
Adobe Acrobat
Apple OS X (120 -140)
Blackberry (lol)
Cisco Devices
Google Chrome
IBM Devices

Java Runtime Environment
MS SQL Server
Microsoft Word/Excel/Access
Firefox
Oracle DBs
SO MANY DIFFERENT LINUX DISTROS
Android and Samsung
Solaris

VMware
All versions of Windows

Windows 10 (284)

https://www.stigviewer.com/

UCF STIG Viewer

HOME STIGS DOD 8500 NIST 800-53 COMMON CONTROLS HUB ABOUT Search...

UNCLASSIFIED DISA FSO STIG List

Title

A10 Networks ADC ALG

A10 Networks ADC NDM

AIX 5.3 SECURITY TECHNICAL IMPLEMENTATION GUIDE

AIX 6.1 SECURITY TECHNICAL IMPLEMENTATION GUIDE

APACHE 2.2 Server for UNIX

APACHE 2.2 Server for Windows

APACHE 2.2 Site for UNIX

APACHE 2.2 Site for Windows Security Implementation Guide

APACHE 2.2 Site for Windows

APACHE SERVER 2.0 for Windows

APACHE SERVER 2.2 for Unix

APACHE SERVER 2.2 for Windows

APACHE SITE 2.0 for Unix

APACHE SITE 2.0 for Windows

APACHE SITE 2.2 for Unix

APACHE SITE 2.2 for Windows

STIGs related to CSCI 476

Red Hat Linux 6

STIG - 217976

*The audit system must be configured to audit all use of **setuid** and setgid programs.*

STIGs related to CSCI 476

Red Hat Linux 6

STIG - 217976

*The audit system must be configured to audit all use of **setuid** and setgid programs.*

Set-UID programs can be great… but they can also be exploited

STIGs related to CSCI 476

Red Hat Linux 6

STIG - 217976

*The audit system must be configured to audit all use of **setuid** and setgid programs.*

Set-UID programs can be great… but they can also be exploited

Logging all uses of these types of programs can help monitor for unusual activity or identify malicious events

STIGs related to CSCI 476

Ubuntu 16.04

STIG - 217976

*The Ubuntu operating system must implement **address space layout randomization** to protect its memory from unauthorized code execution.*

.

STIGs related to CSCI 476

Ubuntu 16.04

STIG - 217976

*The Ubuntu operating system must implement **address space layout randomization** to protect its memory from unauthorized code execution.*

.

ASLR is one of the top defenses against buffer overflows *(however enabling ASLR does not mean you are completely immune to buffer overflows)*

Enabling ASLR will help prevent potential overflow attacks

STIGs related to CSCI 476

Application Security and Development Checklist

STIG - 16811

*The designer will ensure the application does not have **cross site scripting (XSS) vulnerabilities**.*

STIG - 16807

*The designer will ensure the application is not vulnerable to **SQL Injection**, uses prepared or parameterized statements, does not use concatenation or replacement to build SQL queries, and does not directly access the tables in a database.*

STIG - 222604

*The application must protect from **command injection**.*

STIGs related to CSCI 476

Red Hat Linux 8

STIG - 230231

RHEL 8 must encrypt all stored passwords with a FIPS 140-2 approved **cryptographic hashing** algorithm.

SHA-256, SHA-512, etc

STIGs related to CSCI 476

Red Hat Linux 8

STIG - 230231

RHEL 8 must encrypt all stored passwords with a FIPS 140-2 approved **cryptographic hashing** algorithm.

Microsoft Office 2013

STIG - 17619

*The **encryption** type for password protected Office 97 - Office 2003 must be set.*

AES 256 & RSA

Compliance rules are not always computer-related

There are often physical aspects of compliance

- Employees wearing badges
- Visitors must be checked in and escorted by an employee
- Doors must remain locked
- Photography must not be allowed

The “level” of security will vary depending on company

Why care?

STIG - 230503

The Red Hat Enterprise Linux operating system must be configured to disable USB mass storage.

STIG - 230231

RHEL 8 must encrypt all stored passwords with a FIPS 140-2 approved **cryptographic hashing** algorithm.

STIG - 16811

*The designer will ensure the application does not have **cross site scripting (XSS) vulnerabilities**.*

STIG - 17619

*The **encryption** type for password protected Office 97 - Office 2003 must be set.*

STIG - 217976

*The audit system must be configured to audit all use of **setuid** and setgid programs.*

STIG - 217976

*The Ubuntu operating system must implement **address space layout randomization** to protect its memory from unauthorized code execution.*

STIG - 16807

*The designer will ensure the application is not vulnerable to **SQL Injection**, uses prepared or parameterized statements, does not use concatenation or replacement to build SQL queries, and does not directly access the tables in a database.*

Why care?

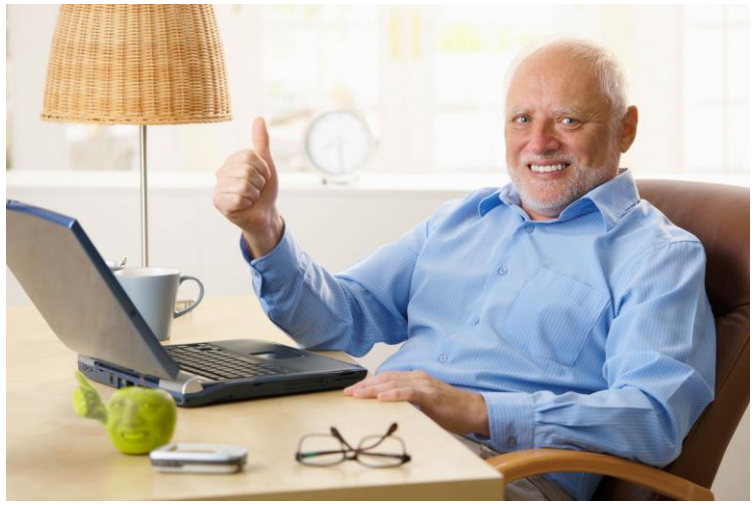
Customers or clients might require the company to be compliant with some framework

Caught violating rules --> hefty fine or termination of contract

Whether or not a company is meeting security requirements is important information to company executives, auditors, or system administrators

Why should we care about Compliance?

If a company is being compliant with their regulatory framework, they are less likely to be a victim of a cyber attack or data breach



Why should we care about Compliance?

If a company is being compliant with their regulatory framework, they are less likely to be a victim of a cyber attack or data breach

How do we go about checking for compliance?

How do we go about checking for compliance?

This process can often be a headache for system administrators….

How do we go about checking for compliance?

STIG - 217976

The Ubuntu operating system must implement ***address space layout randomization*** *to protect its memory from unauthorized code execution.*

.

How do we go about checking for compliance?

STIG - 217976

The Ubuntu operating system must implement ***address space layout randomization*** *to protect its memory from unauthorized code execution.*

.

stig-217976.sh

```
sudo sysctl kernel.randomize_va_space
```

How do we go about checking for compliance?

STIG - 217976

The Ubuntu operating system must implement ***address space layout randomization*** *to protect its memory from unauthorized code execution.*

.

stig-217976.sh

```
sudo sysctl kernel.randomize_va_space
```

```
reese@reese-VirtualBox:~$ sudo sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
reese@reese-VirtualBox:~$
```

How do we go about checking for compliance?

STIG - 217976

The Ubuntu operating system must implement ***address space layout randomization*** *to protect its memory from unauthorized code execution.*

.

stig-217976.sh

```
sudo sysctl kernel.randomize_va_space
```

```
reese@reese-VirtualBox:~$ sudo sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
reese@reese-VirtualBox:~$
```

If it is set to 2, then ASLR is enabled

How do we go about checking for compliance?

STIG - 217976

The Ubuntu operating system must implement ***address space layout randomization*** *to protect its memory from unauthorized code execution.*

.

stig-217976.sh

```
sudo sysctl kernel.randomize_va_space
```

```
reese@reese-VirtualBox:~$ sudo sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
reese@reese-VirtualBox:~$
```

If it is set to 2, then ASLR is enabled

If the output is **not** 2, then this means that ASLR is not enabled, which is a “finding”

How do we go about checking for compliance?

Stigviewer does a good job of explaining the details of this process.

Details

Check Text (C-75509r2_chk)

Verify the Ubuntu operating system implements address space layout randomization (ASLR).

Check that ASLR is configured on the system with the following command:

sudo sysctl kernel.randomize_va_space

kernel.randomize_va_space = 2

If nothing is returned; we must verify the kernel parameter "randomize_va_space" is set to "2" with the following command:

kernel.randomize_va_space" /etc/sysctl.conf /etc/sysctl.d/*

kernel.randomize_va_space = 2

If "kernel.randomize_va_space" is not set to "2", this is a finding.

Fix Text (F-82451r2_fix)

Configure the operating system implement virtual address space randomization.

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" (or modify the line to have the required value):

kernel.randomize_va_space=2

How do we go about checking for compliance?

STIG - 72005

*The Red Hat Enterprise Linux operating system must be configured so that the root account must be the **only** account having unrestricted access to the system.*

```
#!/bin/bash
awk -F: '$3 == 0 {print $1}' /etc/passwd
```

How do we go about checking for compliance?

STIG - 72005

*The Red Hat Enterprise Linux operating system must be configured so that the root account must be the **only** account having unrestricted access to the system.*

```
#!/bin/bash
awk -F: '$3 == 0 {print $1}' /etc/passwd
```

This prints all the User Identifiers on the system that have an UID of 0
If there is an account other than `root` that gets printed out, this is a “finding”

How do we go about checking for compliance?

STIG - 72005

*The Red Hat Enterprise Linux operating system must be configured so that the root account must be the **only** account having unrestricted access to the system.*

```
#!/bin/bash
awk -F: '$3 == 0 {print $1}' /etc/passwd
```

This prints all the User Identifiers on the system that have an UID of 0
If there is an account other than `root` that gets printed out, this is a “finding”

```
reese@reese-VirtualBox:~$ awk -F: '$3 == 0 {print $1}' /etc/passwd
root
reese@reese-VirtualBox:~$
```

How do we go about checking for compliance?

STIG - 72005

*The Red Hat Enterprise Linux operating system must be configured so that the root account must be the **only** account having unrestricted access to the system.*

```
#!/bin/bash
awk -F: '$3 == 0 {print $1}' /etc/passwd
```

STIG - 71983

The Red Hat Enterprise Linux operating system must be configured to disable USB mass storage.

```
#!/bin/bash
grep usb-storage /etc/modprobe.d/* | grep -i "blacklist" | grep -v "^#"
```

How do we go about checking for compliance?

STIG - 72005

*The Red Hat Enterprise Linux operating system must be configured so that the root account must be the **only** account having unrestricted access to the system.*

```
#!/bin/bash
awk -F: '$3 == 0 {print $1}' /etc/passwd
```

STIG - 71983

The Red Hat Enterprise Linux operating system must be configured to disable USB mass storage.

```
#!/bin/bash
grep usb-storage /etc/modprobe.d/* | grep -i "blacklist" | grep -v "^#"
```

This prints out all blacklisted settings. If “blacklist usb-storage” is not printed out, then this is a “finding”

How do we go about checking for compliance?

STIG - 72005

*The Red Hat Enterprise Linux operating system must be configured so that the root account must be the **only** account having unrestricted access to the system.*

```
#!/bin/bash
awk -F: '$3 == 0 {print $1}' /etc/passwd
```

STIG - 71983

The Red Hat Enterprise Linux operating system must be configured to disable USB mass storage.

```
#!/bin/bash
grep usb-storage /etc/modprobe.d/* | grep -i "blacklist" | grep -v "^#"
```

This prints out all blacklisted settings. If “blacklist usb-storage” is not printed out, then this is a “finding”

```
reese@reese-VirtualBox:~$ grep usb-storage /etc/modprobe.d/* |grep -i "blacklis
t" | grep -v "^#"
reese@reese-VirtualBox:~$
```

How do we go about checking for compliance?

STIG - 72005

*The Red Hat Enterprise Linux operating system must be configured so that the root account must be the **only** account having unrestricted access to the system.*

```
#!/bin/bash
awk -F: '$3 == 0 {print $1}' /etc/passwd
```

STIG - 71983

The Red Hat Enterprise Linux operating system must be configured to disable USB mass storage.

```
#!/bin/bash
grep usb-storage /etc/modprobe.d/* | grep -i "blacklist" | grep -v "^#"
```

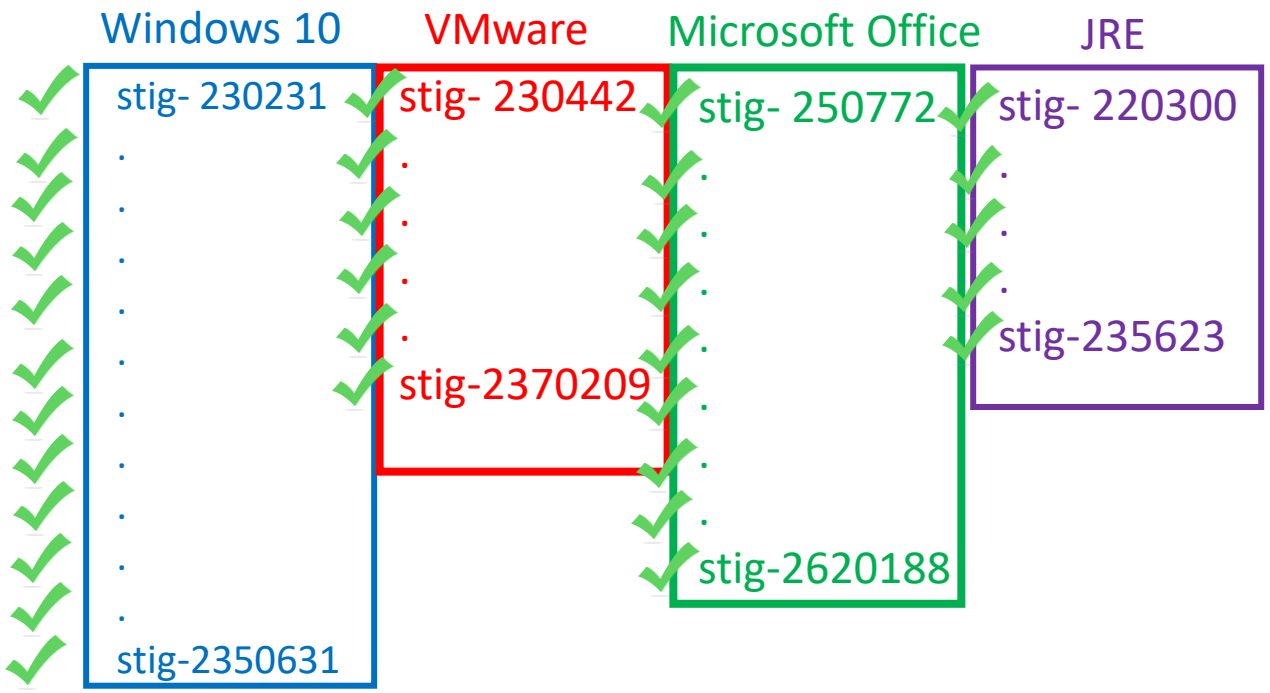
This prints out all blacklisted settings. If “blacklist usb-storage” is not printed out, then this is a “finding”

```
reese@reese-VirtualBox:~$ grep usb-storage /etc/modprobe.d/* |grep -i "blacklis
t" | grep -v "^#"
reese@reese-VirtualBox:~$
```

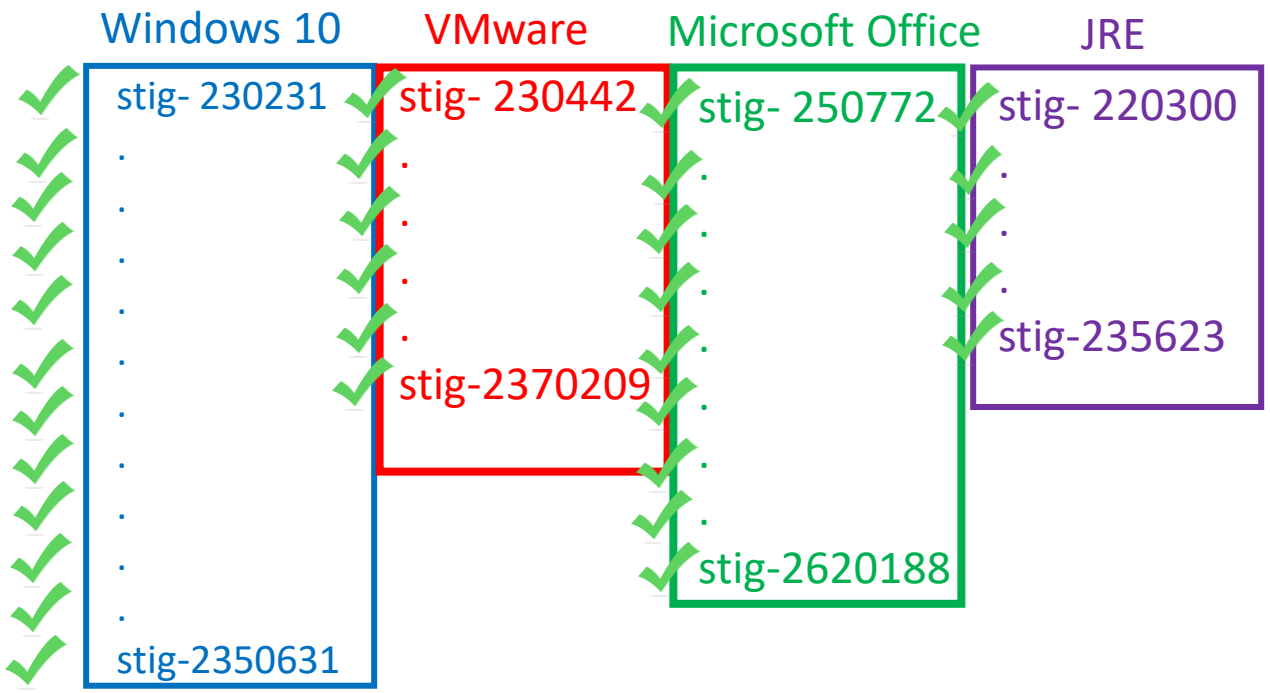
How do we go about checking for compliance?

Windows 10	VMware	Microsoft Office	JRE
stig- 230231	stig- 230442	stig- 250772	stig- 220300
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	stig-235623
.	stig-2370209	.	
.		.	
.		.	
.		.	
.		stig-2620188	
.			
stig-2350631			

How do we go about checking for compliance?



How do we go about checking for compliance?



Then we can say we are STIG-compliant and less likely to be victim of some kind of cyber attack or breach

Conclusion

Compliance is one of the many ways we implement security controls in industry

There are many different **compliance frameworks** that provide standards and rules to help mitigate cyber risks

- The things you learned in CSCI 476 are legitimate concerns that are addressed in these frameworks!

As you go into the workforce and industry, you will likely have to go through some kind of compliance training

Thank you for listening!

And good luck on your final lab!

Any questions?

Compliance, Security, Grad School, Careers, etc

reesepearsallcs@gmail.com