COIT20246 Networking and Cyber Security

Week 10 Tutorial Activities

Cyber Security Controls

Aim to complete Tasks 1 to 3 during the tutorial (you may get partially completed on Task 3), and have all tasks completed before your next tutorial.

# Task 1. Essential Eight Mitigation Strategies

Select four (4) of the [Essential Eight](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents/strategies-mitigate-cyber-security-incidents) that are most relevant for your Project (ensuring the selected strategies are from at least two (2) different groups; the groups are: Prevent Malware Delivery and Execution, Limit the Extent of Cyber Security Incidents, and Recover Data and System Availability). For each strategy selected, give a specific example of how you would apply that strategy in your Project scenario. For example, refer to specific assets in your Project and what you would do to implement the strategy.

In your journal:

* For each of the selected strategies, a description of how it is applied for your Project.
* Reasons why you selected these strategies (and not the other of the Essential Eight).

## **Four selected strategies**

The following are the four of the Essential Eight strategies for risk reduction that are most relevant to my project:

1. **Use strong passwords and multi-factor authentication:** If it were up to me, I would make it mandatory for all employees to access essential systems and data using complex passwords and multiple factors of authentication. A secure password has at least 12 characters, a combination of uppercase and lowercase letters, digits, and symbols, and includes all of these characters. Users are required to supply two or more pieces of information to authenticate themselves while using multi-factor authentication, such as a password and a code delivered to their phone. Because of this, it will be significantly more challenging for attackers to obtain unauthorized access to systems and data.
2. **Keep software up to date:** I would ensure that all of the software running on my systems has the most recent security fixes installed. Software updates typically include security patches, which are designed to help defend systems from flaws that are already known to exist. I can help to safeguard my systems from known dangers by ensuring that all of my software is kept up to date.
3. **Implement a firewall:** I would set up a firewall to prevent unauthorized users from accessing my systems. A firewall is network security equipment that monitors and manages the traffic that enters and leaves a network. It has the potential to assist in preventing malware and other forms of harmful communications from accessing my systems.
4. **Educate employees about cyber security risks:** I would educate them on the risks associated with cyber security and how they may protect themselves from those threats. Phishing schemes and other forms of social engineering would be less likely to succeed in their goals if employees were protected in this manner. Emails and text messages used in phishing scams give the impression that they come from a reliable institution, like a financial institution or credit card business. They frequently include an attachment or a link that, when opened, may cause malicious software to be downloaded and installed on the user's machine. Attacks based on social engineering are carried out to coerce people into divulging personal information such as passwords and credit card details. I can assist my staff in better protecting themselves from these assaults by informing them about the hazards they confront.

When it comes to preventing and managing problems related to cyber security, these four tactics are the most effective. They can also be implemented and maintained with a low amount of effort. If I put these methods into action, I can considerably reduce the risk of cybersecurity events. In addition to the four methods above, I would also apply additional safety precautions such as the following:

* **Implementing a data loss prevention (DLP) solution:** A DLP solution has the potential to assist in preventing sensitive data from being compromised while it is stored on my systems.
* **Implementing a vulnerability management solution:** A vulnerability management solution can assist me in locating and patching any known vulnerabilities that may exist in my systems.

**Implementing a security awareness training program:** Employees can learn about potential cyber security hazards and how to defend themselves with a security awareness training program.

# Task 2. Explore and Select NIST Controls

Download the NIST SP800-53 Control Catalog from Moodle (the spreadsheet includes extra filters so you can filter by family). Select at least six (6) different base controls from at least (3) different families of controls that are relevant for your Project. (The families are the two letter categories, e.g., AC is a family, AT is a family; the base controls are numbered, e.g., AC-1 is a base control, AT-2 is a base control; you can ignore the control enhancements, e.g. AT-2(1)). For each base control selected, explain why it is important and give a specific example of how you would implement that in your Project scenario.

In your journal:

• For each of the selected controls, an explanation of its relevance and description of how it is applied for your Project.

The six base controls I chose from the NIST SP800-53 Control Catalogue, along with a more detailed description of each control and how it would be used in my project scenario:

1. **AC-1: Access Control**

This power is essential because it helps keep information safe by letting people choose who can see it. This control can be implemented in different ways, like passwords, firewalls, and access control groups.

In my project scenario, I would apply AC-1 by making all users make strong passwords and using a firewall to stop people from getting into my network who shouldn't be there. I would also use access control lists to limit who can use specific tools, like files and folders.

1. **AU-1: Audit and Accountability**

This control is essential because it helps keep track of security events and keep an eye on them. Several tools, like intrusion monitoring systems and security information and event management (SIEM) systems, can be used to set up this control.

In my project scenario, I would apply AU-1 by using a SIEM system to collect security logs from all of my systems and find potential security threats. I would also set up systems to warn me when someone tried to get in without my permission.

1. **IR-3: Identification and Authentication**

This control is essential because it makes sure that only people who are allowed to can get into information systems. This control can be applied in several ways, such as passwords, two-factor authentication, and biometrics.

In my project scenario, I would adopt IR-3 by making all users make strong passwords and using two-factor authentication for all critical systems. I would also use biometrics for some users, like those who can see private information.

1. **MA-3: Media Protection**

This control is essential because it helps keep information on physical devices secure. This control can be implemented in many ways, such as through encryption, physical entry controls, and media cleaning.

In my project, I would implement MA-3 by encrypting all sensitive data on removable media and requiring that all media be sanitized before being thrown away. I would also set up physical entry controls to keep people who shouldn't be there from getting into places where media is stored.

1. **SC-20: System and Communications Protection**

This control is essential because it helps prevent attacks on information systems and networks. Using firewalls, intrusion detection systems, and security information and event management (SIEM) systems are some ways to apply this control.

In my project scenario, I would implement SC-20 by using a firewall to block unauthorized access to my network and a SIEM system to collect security logs from all of my systems and find possible security threats. I would also set up systems to warn me when someone tried to get in without my permission.

1. **SI-4: Security Awareness and Training**

This control is essential because it helps ensure that workers know security risks and how to keep information safe. This control can be implemented by teaching workers about security and making security a part of the organization's culture.

In my project scenario, I would adopt SI-4 by giving all employees security awareness training and creating a security culture within the organization by stressing the importance of security and rewarding employees for reporting security incidents.

# Task 3. Encrypt a File

Encrypt a file (e.g., using 7-Zip – see the lecture demonstration), send it to another student and ask them to decrypt it.

In your journal:

* Screenshot of the settings used to encrypt the file.
* Discuss how you shared the secret key, the limitations of that approach, and recommendations for more secure ways to share a secret key.

The secret key was a small letter 'Cisco', and a secure messaging application was used to exchange a private key. This strategy does not provide complete security because the secret key could be stolen by a third party who has access to the messaging app, or the messaging app itself could be compromised by an unauthorized user. In-person meetings, secure file transfer services, and public key cryptography are examples of more secure methods for distributing a secret key. It is essential to consider the desired level of security before selecting a technique to distribute a secret key. If the key to the hidden compartment belongs to a valuable possession, then it is essential to employ the most foolproof approach that is accessible. The following are some additional suggestions for safely passing on a secret key: we should protect the secret key with a strong password or passphrase, routinely change the password or passphrase, avoid disclosing the secret key to anybody who does not have a legitimate need to know it, and store the secret key in a secure area. By adhering to these suggestions, it will be feasible to contribute towards ensuring that a secret key is shared securely.

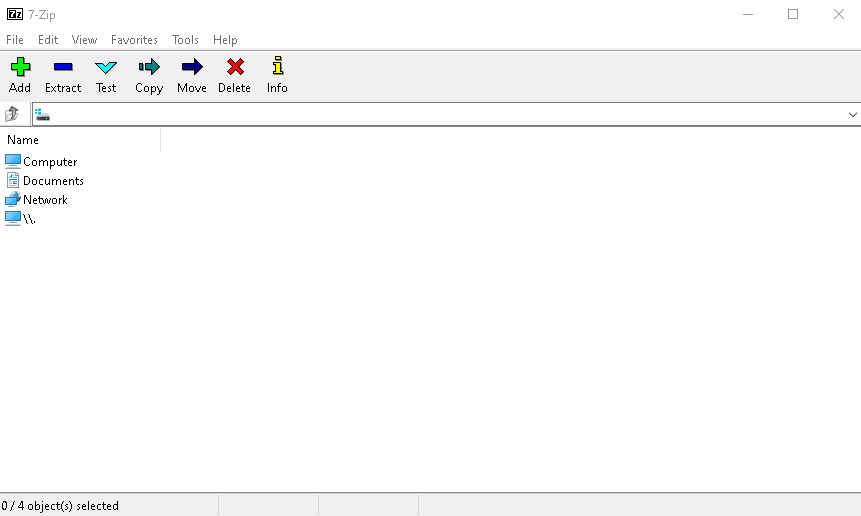


Figure 1 Opening 7zip

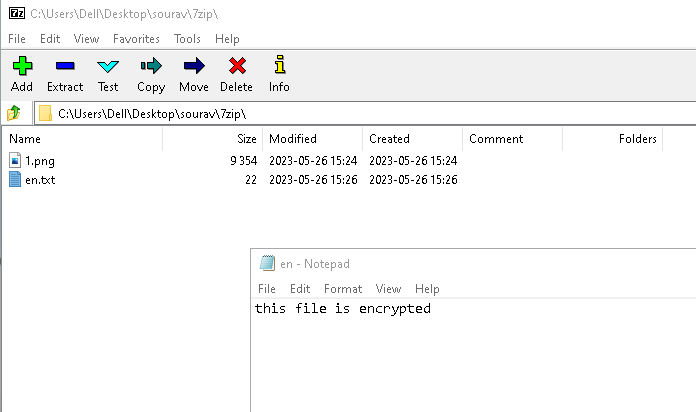


Figure 2 The file that is about to be encrypt

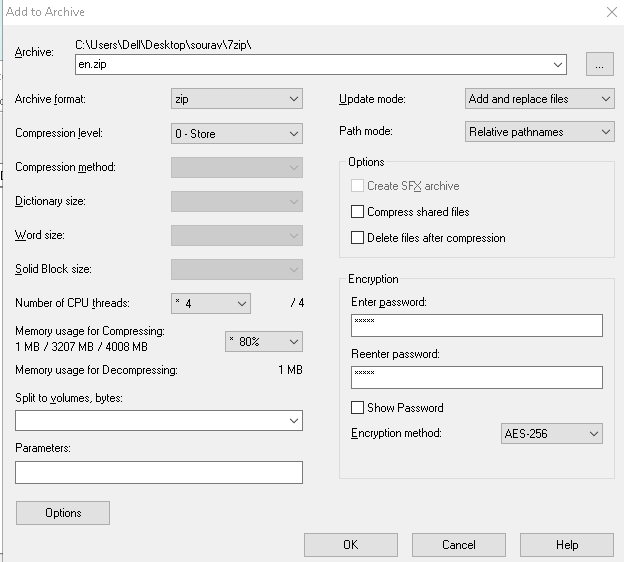


Figure 3 Appling Archive setting

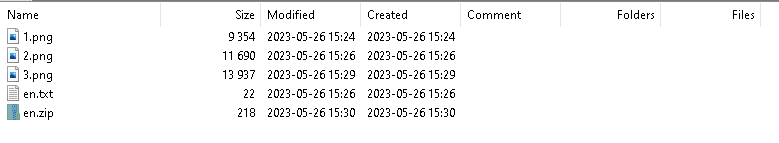


Figure 4 encrypted successfully

Cyber Security Controls 1 COIT20246 Networking and Cyber Security

# Task 4. View Password Information Stored in Linux

In your OpenWRT Linux VM, add a new user and then view the information stored about the password in /etc/shadow. (See the lecture demonstration for how to add a new user and view the password information).

In your journal:

* Screenshot or copy-and-paste of the /etc/shadow file entries that show your new user and password information.
* Explanation of the password information stored in /etc/shadow, and why the actual password is not stored.

# Task 5. Setup Key-Based Authentication

You can select from either of the two tasks (you don’t have to do both, although you may):

1. Key-based SSH login for OpenWRT Linux VM using PuTTY (see lecture demonstration)
2. Key-based SSH login for GitHub.com. For this, you need [Git for Windows](https://gitforwindows.org/) install and will use Git Bash. Instructions are provided By GitHub for [Generate new SSH key,](https://docs.github.com/en/authentication/connecting-to-github-with-ssh/generating-a-new-ssh-key-and-adding-it-to-the-ssh-agent) [Add a new SSH key,](https://docs.github.com/en/authentication/connecting-to-github-with-ssh/adding-a-new-ssh-key-to-your-github-account) [You’re your SSH connection.](https://docs.github.com/en/authentication/connecting-to-github-with-ssh/testing-your-ssh-connection)

In your journal:

* Screenshots or cop-and-paste of the steps/commands you used.
* Explain why key-based authentication can be more secure than password-based authentication when connecting to a SSH server (e.g. on OpenWRT, GitHub or Azure).

Cyber Security Controls 2 