Please watch this YouTube link first to get an understanding of the assignment…

YouTube Link: <https://youtu.be/rStxKMeGXAI>

The security posture of the information systems infrastructure of an organization should be regularly monitored and assessed (including software, hardware, firmware components, governance policies, and implementation of security controls). The monitoring and assessment of the infrastructure and its components, policies, and processes should also account for changes and new procurements that are sure to follow in order to stay in step with ever-changing information system technologies.

The data breach at the Office of Personnel Management (OPM) is one of the largest in US government history. It provides a series of lessons learned for other organizations in industry and the public sector. Some critical security practices, such as lack of diligence to security controls and management of changes to the information systems infrastructure were cited as contributors to the massive data breach in the OPM Office of the Inspector General's (OIG) Final Audit Report, which can be found in open source searches. Some of the findings in the report include: weak authentication mechanisms; lack of a plan for life-cycle management of the information systems; lack of a configuration management and change management plan; lack of inventory of systems, servers, databases, and network devices; lack of mature vulnerability scanning tools; lack of valid authorizations for many systems, and lack of plans of action to remedy the findings of previous audits.

The breach ultimately resulted in removal of OPM's top leadership. The impact of the breach on the livelihoods of millions of people is ongoing and may never be fully known. There is a critical need for security programs that can assess vulnerabilities and provide mitigations.

**Step 1: Enterprise Network Diagram**

During Project One, you researched a hypothetical or actual organization of your choice. You had to understand the goals of the organization and the types of systems that would fulfill those goals. You will now research and learn about types of networks and their secure constructs that may be used in organizations to accomplish the functions of the organization’s mission. You will propose a local area network (LAN) and a wide area network (WAN) for the organization, define the systems environment, and incorporate this information in a network diagram. Discuss the security benefits of your chosen network design.

Read about the following computing platforms available for networks and discuss how these platforms could be implemented in your organization. Include the rationale for all platforms you choose to include in your network design.

* [common computing platforms](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Common%20Computing%20Platforms)
* [cloud computing](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Cloud%20Computing)
* [distributed computing](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Distributed%20Computing)
* [centralized computing](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Centralized%20Computing)
* [secure programming fundamentals](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Secure%20Programming%20Fundamentals)

# Step 2: Enterprise Threats

Review the OIG report on the OPM breach that you were asked to research and read about at the beginning of the project. The OIG report included numerous security deficiencies that likely left OPM networks vulnerable to being breached. In addition to those external threats, the report also describes the ways OPM was vulnerable to insider threats. The information about the breach could be classified as threat intelligence. Define threat intelligence and explain what kind of threat intelligence is known about the OPM breach.

You just provided detailed background information on your organization. Next, you’ll describe threats to your organization’s system. Before you get started, select and explore the contents of the following link: [insider threats](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Insider%20Threats) (also known as internal threats). As you’re reading, take note of which insider threats are a risk to your organization.

Now, differentiate between the external threats to the system and the insider threats. Identify where these threats can occur in the previously created diagrams. Relate the OPM threat intelligence to your organization. How likely is it that a similar attack will occur at your organization?

# Step 3: Scanning the Network

**Note:** You will use the tools in Workspace for this step. If you need help outside the classroom to complete this project, register for CLAB 699 Cyber Computing Lab Assistance (go to the Discussions List for registration information). Primary lab assistance is available from a team of lab assistants. Lab assistants are professionals and are trained to help you.

Click here to access the instructions for [Navigating the Workspace and the Lab Setup](https://content.umuc.edu/file/23b4d73e-dc4e-4907-a24d-de3330d03631/1/UMUCDigitalLabsRev2.pdf).

Select the following link to enter [Workspace](http://virtualdesktop.umuc.edu/). and complete the lab activities related to network vulnerabilities.

You will now investigate network traffic, and the security of the network and information system infrastructure overall. Past network data has been logged and stored, as collected by a network analyzer tool such as Wireshark. Explore the tutorials and user guides to learn more about the tools you will use. Click the following link to read more about these network monitoring tools: [Tools to Monitor and Analyze Network Activities](https://umuc.equella.ecollege.com/file/f634286e-5b85-4e39-a6b5-b785a36ec2cc/1/launch.html).

You will perform a network analysis on the Wireshark files provided to you in Workspace and assess the network posture and any vulnerability or suspicious information you are able to obtain. Include this information in the SAR.

You will then return to the lab in order to identify any suspicious activities on the network, through port scanning and other techniques. You will revisit the lab and lab instructions in Step 7: Suspicious Activity.

Click here to access the [Project 3 Workspace Exercise Instructions](https://umuc.equella.ecollege.com/file/f634286e-5b85-4e39-a6b5-b785a36ec2cc/2/CYB610Project3Lab.pdf).

In order to validate the assets and devices on the organization's network, run scans using security and vulnerability assessment analysis tools such as MBSA, OpenVAS, Nmap, or Nessus depending on the operating systems of your organization's networks. Live network traffic can also be sampled and scanned using Wireshark on either the Linux or Windows systems. Wireshark allows you to inspect all OSI layers of traffic information. Further analyze the packet capture for network performance, behavior, and any suspicious source and destination addresses on the networks.

In the previously created Wireshark files, identify if any databases had been accessed. What are the IP addresses associated with that activity? Include this information in the SAR.

# Step 4: Identifying Security Issues

You have a suite of security tools, techniques, and procedures that can be used to assess the security posture of your organization's network in a SAR.

Now it's time to identify the security issues in your organization's networks. You have already used password cracking tools to crack weak and vulnerable passwords. Provide an analysis of the strength of passwords used by the employees in your organization. Are weak passwords a security issue for your organization?

# Step 5: Firewalls and Encryption

Next, examine these resources on [firewalls](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Firewalls) and [auditing–RDBMS](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Auditing%20-%20RDBMS) related to the use of the Relational Database Management System (i.e., the database system and data) RDBMS. Also review these resources related to [access control](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Access%20Control).

Determine the role of firewalls and encryption, and auditing – RDBMS that could assist in protecting information and monitoring the confidentiality, integrity, and availability of the information in the information systems.

Reflect any weaknesses found in the network and information system diagrams previously created, as well as in the developing SAR.

**Step 6: Threat Identification**

You know of the weaknesses in your organization's network and information system. Now you will determine various known threats to the organization's network architecture and IT assets.

Get acquainted with the following types of threats and attack techniques. Which are a risk to your organization?

* IP address [spoofing/cache poisoning attacks](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Spoofing/Cache%20Poisoning%20Attacks)
* [denial of service attacks](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Denial%20of%20Service%20Attacks%20(DoS)) (DoS)
* [packet analysis/sniffing](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Packet%20Analysis/Sniffing)
* [session hijacking attacks](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Session%20Hijacking%20Attacks)
* [distributed denial of service attacks](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Distributed%20Denial%20of%20Service%20Attacks)

In identifying the different threats, complete the following tasks:

1. Identify the potential hacking actors of these threat attacks on vulnerabilities in networks and information systems and the types of remediation and mitigation techniques available in your industry, and for your organization.
2. Identify the purpose and function of firewalls for organization network systems, and how they address the threats and vulnerabilities you have identified.
3. Also discuss the value of using access control, database transaction and firewall log files.
4. Identify the purpose and function of encryption, as it relates to files and databases and other information assets on the organization's networks.

Include these in the SAR.

# Step 7: Suspicious Activity

**Note:** You will utilize the tools in Workspace for this step.

Hackers frequently scan the Internet for computers or networks to exploit. An effective firewall can prevent hackers from detecting the existence of networks. Hackers continue to scan ports, but if the hacker finds there is no response from the port and no connection, the hacker will move on. The firewall can block unwanted traffic and NMap can be used to self-scan to test the responsiveness of the organization's network to would-be hackers.

Select the following link to enter [Workspace](http://virtualdesktop.umuc.edu/) and conduct the port scanning. Return to the lab instructions by clicking here to access the [Project 3 Workspace Exercise Instructions](https://umuc.equella.ecollege.com/file/f634286e-5b85-4e39-a6b5-b785a36ec2cc/2/CYB610Project3Lab.pdf).

# Step 8: Risk and Remediation

What is the risk and what is the remediation? What is the security exploitation? You can use the OPM OIGFinal Audit Report findings and recommendations as a possible source for methods to remediate vulnerabilities.

Read this [risk assessment](https://lti.umuc.edu/contentadaptor/page/topic?keyword=Risk%20Assessment) resource to get familiar with the process, then prepare the risk assessment. Be sure to first list the threats, then the vulnerabilities, and then pairwise comparisons for each threat and vulnerability, and determine the likelihood of that event occurring, and the level of impact it would have on the organization. Use the OPM OIG Final Audit Report findings as a possible source for potential mitigations. Include this in the risk assessment report (RAR).

**Step 9: Creating the SAR and RAR**

Your research and Workspace exercise have led you to this moment: creating your SAR and RAR. Consider what you have learned in the previous steps as you create your reports for leadership.

Prepare a Security Assessment Report (SAR) with the following sections:

1. Purpose
2. Organization
3. Scope
4. Methodology
5. Data
6. Results
7. Findings

The final SAR does not have to stay within this framework, and can be designed to fulfill the goal of the security assessment.

Prepare a Risk Assessment Report (RAR) with information on the threats, vulnerabilities, likelihood of exploitation of security weaknesses, impact assessments for exploitation of security weaknesses, remediation, and cost/benefit analyses of remediation. Devise a high-level plan of action with interim milestones (POAM), in a system methodology, to remedy your findings. Include this high-level plan in the RAR. Summarize the results you obtained from the vulnerability assessment tools (i.e., MBSA and OpenVas) in your report.

The deliverables for this project are as follows:

1. Security Assessment Report (SAR): This should be an 8-10 page double-spaced Word document with citations in APA format. The page count does not include figures, diagrams, tables, or citations.
2. Risk Assessment Report (RAR): This report should be a 5-6 page double-spaced Word document with citations in APA format. The page count does not include figures, diagrams, tables, or citations.