**Project 3 Start Here**

[Transcript](https://umuc.equella.ecollege.com/file/f634286e-5b85-4e39-a6b5-b785a36ec2cc/1/CYB610Project3.pdf)

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.

There are 10 steps that will lead you through this project. You should complete Project 3 during Weeks 2-5. After beginning with the workplace scenario, continue to Step 1: "Organizational Background."

When you submit your project, your work will be evaluated using the competencies listed below. You can use the list below to self-check your work before submission.

* 1.1: Organize document or presentation in a manner that promotes understanding and meets the requirements of the assignment.
* 1.2: Develop coherent paragraphs or points to be internally unified and function as part of the whole document or presentation.
* 1.3: Provide sufficient, correctly cited support that substantiates the writer’s ideas.
* 1.4: Tailor communications to the audience.
* 1.5: Use sentence structure appropriate to the task, message and audience.
* 1.6: Follow conventions of Standard Written English.
* 5.2 Enterprise Architecture: Knowledge of architectural methodologies used in the design and development of information systems, including the physical structure of a system's internal operations and interactions with other systems and knowledge of stan
* 5.6: Technology Awareness: Explore and address cybersecurity concerns, promote awareness, best practice, and emerging technology
* 7.3: Risk Management : Knowledge of methods and tools used for risk management and mitigation of risk
* 8.1: Incident Detection: Demonstrate the abilities to detect, identify, and resolve host and network intrusion incidents.
* 8.2: Incident Classification: Possess knowledge and skills to categorize, characterize, and prioritize an incident as well as to handle relevant digital evidence appropriately.

**Step 1: Organizational Background**

Perform quick independent research on organizational structure in your industry sector. Describe the background of your organization, including the purpose, organizational structure, the network system description, and a diagram of the organization. Include LAN, WAN, and systems in diagram format, the intra-network, and WAN side networks, and the internet. Identify the boundaries that separate the inner networks from the outside networks. Take time to click on and read about the following computing platforms available for networks, then include a description of how these platforms are implemented in your organization:

* common computing platforms
* cloud computing
* distributed computing
* centralized computing
* secure programming fundamentals

This information can be fictitious, or modeled from existing organizations. Be sure to cite references.

# Step 2: Organizational Threats

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 (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. Define threat intelligence, and explain what kind of threat intelligence is known about the OPM breach. 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 utilize the tools in Workspace for this step. If you need help outside the classroom to complete this project, you must 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 [Project 3 Workspace Exercise Instructions](https://umuc.equella.ecollege.com/file/f634286e-5b85-4e39-a6b5-b785a36ec2cc/2/CYB610Project3Lab.pdf). Explore the tutorials and user guides to learn more about the tools you will use. You will perform this lab in Step 7.

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 (we do this in step 7) on either the Linux or Windows systems. Wireshark allows you to inspect all OSI Layers of traffic information. 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).

Provide the report as part of the SAR.

Review the information captured in these two links message and protocols and Transmission Control Protocol/Internet Protocol (TCP/IP), and identify any security communication, message and protocols, or security data transport methods used such as (TCP/IP), SSL, and others. Make note of this, as it should be mentioned in your reports.

# 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 and auditing–RDBMS 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.

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
* denial of service attacks (DoS)
* packet analysis/sniffing
* session hijacking attacks
* distributed denial of service attacks

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: Network Analysis

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

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.

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

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. 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 8: 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. Provide your findings in the SAR deliverable. Provide analyses of the scans and any recommendation for remediation, if needed. Identify any suspicious activity and formulate the steps in an incidence response that could have been, or should be, enacted. Include the responsible parties that would provide that incidence response and any follow-up activity. Include this in the SAR. Please note that some scanning tools are designed to be undetectable. While running the scan and observing network activity with Wireshark, attempt to determine the detection of the scan in progress. If you cannot identify the scan as it is occurring, indicate this in your SAR.

# Step 9: Risk and Remediation

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

Read this risk assessment 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 10: 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.
3. In a Word document, share your lab experience and provide screen prints to demonstrate that you performed the lab.

Submit your deliverables to the assignment folder.

Before you submit your assignment, review the competencies below, which your instructor will use to evaluate your work. A good practice would be to use each competency as a self-check to confirm you have incorporated all of them in your work.

* 1.1: Organize document or presentation in a manner that promotes understanding and meets the requirements of the assignment.
* 1.2: Develop coherent paragraphs or points to be internally unified and function as part of the whole document or presentation.
* 1.3: Provide sufficient, correctly cited support that substantiates the writer’s ideas.
* 1.4: Tailor communications to the audience.
* 1.5: Use sentence structure appropriate to the task, message and audience.
* 1.6: Follow conventions of Standard Written English.
* 5.2 Enterprise Architecture: Knowledge of architectural methodologies used in the design and development of information systems, including the physical structure of a system's internal operations and interactions with other systems and knowledge of stan
* 5.6: Technology Awareness: Explore and address cybersecurity concerns, promote awareness, best practice, and emerging technology
* 7.3: Risk Management : Knowledge of methods and tools used for risk management and mitigation of risk
* 8.1: Incident Detection: Demonstrate the abilities to detect, identify, and resolve host and network intrusion incidents.
* 8.2: Incident Classification: Possess knowledge and skills to categorize, characterize, and prioritize an incident as well as to handle relevant digital evidence appropriately.

Basically, you are going to have a network diagram that shows the different levels of the network (backend, intranet, DMZ, frontend applications, etc) all the way through to the internet. Show how you are separating the logical portions (firewalls, switches, VLANs, etc).