# SEC555 – Cybersecurity – Summer 2024

Term Project – 20% of final grade

## Overview of Tasks and Instructions

1. Find a partner (preferably in your lab section) and give yourselves a group name.
   1. You may work alone if you chose but no groups larger than 2​.
   2. Sign up your group on blackboard
   3. Your project partner must be in your lab period
   4. Even if you work alone, give yourself a group name.

​

1. In a virtual environment, install and configure a Vulnerability Scanner on the Kali system which you will use to identify weaknesses on your target system (Metasploitable)​.
   1. Nessus, Greenbone, Nexpose are all available open-source​.

​

1. Using the skills learned in Labs A-E you will act as an attacker AND the defender for your environment. This is your Security INCIDENT for your presentation.
   1. Build your lab environment. You may use the VMs that you have been using all semester.
      1. You may build a new Kali system or use the one from the lab.
      2. You may also import a new Windows 10 if you wish to keep things clean. If you install new Windows 10, do not forget to tool it for defense (Security onion agent etc.)
      3. Make sure your windows VM and attacker System VM have Unique hostnames (We recommend you name them after your group)
      4. If you create any kind of call back mechanic (e.g. Using DNS) ensure you are using a unique domain name. We recommend using “<groupname>.lan” as your domain (like we used kali.lan in the lab)
   2. Select a new C2 tool from <https://howto.thec2matrix.com/> you may NOT use Sliver as your C2 since we used it in lab. Make sure whatever C2 you select, you are able to meet the requirements of the project (remote code execution on the endpoint)
   3. Attack the client. You may construct a story on how this happens. Simulate email, a file download, opening an attachment, etc. Anything that you consider plausible. If you need to install other software in your Windows 10 System to construct your story, do so (e.g. Installing office to show infected word document).
      1. Are you able to get persistence? If so, how?
   4. Disable Antivirus if you need to. Anti-virus bypass is NOT IN SCOPE for the project.
   5. Once your payload executes on your target system, prove you have remote code execution
      1. In your project presentation include a screenshot from your ATTACKER system showing that you obtained remote code execution on your windows PC.
      2. An effective way to prove you have RCE is showing what username you are running as and the hostname of the target system FROM your attacker system. This is important and will be heavily weighted in the grading.
   6. Identify your malicious traffic using screenshots from security onion
      1. Take screenshots from security onion showing anything you can learn “as the defender” about your attacker and the system they attacked. E.g. from security onion, can you identify the C2 that was used?
      2. Can you identify the way the system was infected?
   7. Clean up the attack as if you were an incident responder

​

## Deliverables and Rubric

1. Vulnerability Scan Report of your Metasploitable target system (**5%**)​
   1. Must be in PDF format and include system details and the date/time the scan was performed​.
   2. Must document in detail each vulnerability discovered by exporting a report from your Vulnerability Scanning solution.

​

1. Presentation including visual media documenting the state of your environment as if you were a SOC (Security Operations Center) member. Ensure you include all of the below information. When you present it, you will need to focus on the most important parts (**50% - Content**)​
   1. What are the most **CRITICAL vulnerabilities** that need to be addressed in the environment (tip, you already have the vulnerability report)
      1. How would you fix these issues?
   2. Summary of the C2 solution that you chose.
   3. As the attacker
      1. Include **screen recording** of the attacker functioning in your PPT presentation – be mindful of the length, you can **skip the video** during your in-person presentation.
   4. As the Defender:
      1. Summary of “The Incident”
      2. The story of how the attacker infected the target system.
         1. What did the attacker do? Include screenshots and proof from your EDR (Endpoint Detection and Response) (Security Onion)
         2. What are the indicators of compromise for the infected workstation (**MD5s, IP addresses, hostnames**) that we would use to find other infected workstations if this was a larger company.
         3. How you cleaned up the attack.
         4. Was the attacker able to get persistence? Did you clean it?
   5. **Make sure that every statement you make about the attacker, or the defender is accompanied by a screenshot PROVING it**. Screenshots should include your group name embedded in the system (hostnames, domain names, virtual machine name, etc.).

**IMPORTANT NOTE**: Marks will be awarded based on the quality of your attacker and defense narrative. Missing components

1. PowerPoint structure and style (**10%**)​
   1. Title page with group name and members​.
   2. Spelling and grammar​.
   3. Professional presentation
   4. Look and polish of your slides​.
   5. References cited in APA (end of deck).​
      1. **Cite ALL sources used.** Plagiarism will NOT be tolerated!! NO copying from other students/groups!! See addendum for Course/College Policies.

​

1. Demonstration of knowledge based on discussion with instructor during your presentation. (**35%**)​
   1. Your group’s timeslot is used to do your presentation AND host questions from the instructor. **Your timeslot includes BOTH the presentation time AND time for questions from the professor.** Make sure that your presentation time fits within the timeslot (10 mins total including questions. You should aim for 7 mins MAX in your presentation period.
   2. Focus on the most important parts of the project and talk about the things you learned in this exercise.
   3. Your entire group must present your PPT project​.
      1. **Each person may be called upon about their findings,** so ensure all group members are comfortable with the material.
   4. You will be asked questions and judged on your understanding of the attack/fix.

## Due Dates

1. Group Members and Group Name
   1. Due June 28nd @ 11:59 PM​
   2. Your project partner must be in your lab period,
   3. Group is signed on blackboard

​

1. PowerPoint Presentation and Vulnerability Scan Report (cumulative 65%)​
   1. To be uploaded by July 26th @ 11:59 PM
   2. Online submission via Blackboard​. Must be in PPTx format (powerpoint default format). PDF submissions will be considered INCOMPLETE
   3. **No** late submissions​.

​

1. In-person group Presentations (35%)​
   1. Presentation schedule will be posted during July 26th to July 29th.
   2. Presentations will occur during your lab period on Week 13 or 14

## Important Information, Resources and Notes

1. You have dedicated lab time in Weeks 10, 11, and 12 to come in and work on your project and/or ask questions. Open Lab times are also posted . Both A4088 or A4081 should have the right permissions for you to work on your labs.
2. VMware licenses have been requested each student; you will receive an email from Brightspace once ITS has configured your license. You MUST use VMware Workstation 17 for compatibility with the Lab PCs in A4081.
3. A companion guide has been documented and posted along with this document on Blackboard.
   1. The companion document provides you with core instructions from Labs A-E.
   2. The companion document will provide you with some resources that you MAY find useful. You should use other resources you find as well.
   3. **This project will require you to do research, learn a new tool, and build your own lab to explore this tool.** You should be comfortable doing all these tasks.
4. The VMs provided during Labs A-E should be used as your environment in the project. If you wish to start from fresh VMs, you may re-download the Lab VMs from the lab file share or get them from you instructor during lab period.
   1. Feel free to customize your VMs as is necessary to tell your Attacker and Defender story, as long as they meet the project requirements. Make sure that your VMs are uniquely identifiable as yours in **ALL** of your screenshots
5. You may download other hacking tools and systems, but **they must ONLY be used within the confines of your virtual environment**. You should also be aware of what those tools do before you download and run them, as malicious payloads can find their way into tools like this. Running everything inside a virtualized environment will help protect your workstations, laptops, and the College’s network but ultimately it is your responsibility to know what you download and run.
6. **VyOS must be turned ON** for the virtual networking to function properly.
   1. It is recommended you statically assign IP addresses to any new VMs added to the environment as it will make your demonstration more reliable.
   2. If necessary, feel free to edit the VyOS configuration to suit your environment. E.g. If you need new DNS records to make your environment work correctly, you may add them.
7. In your lab, all of your systems should be deployed in such a way that they have Internet access. This is true of all the systems as of the end of Lab E however if you modify any of your networking to bring up new systems, those systems should not interfere with the existing environment.