Cybersecurity Website Hardening Project – Team 3

Report Week: 11/10 to 11/17

Status: Green, Yellow, or Red:

Green

Progress summary:

Completed Milestone 3 and submitted an updated poster, flash video, and presentation video for C-day.

Meeting Summary:

This week we had four meetings. On Monday, we had rehearsals for our milestone 3 presentation. Our milestone 3 Presentation took place on Tuesday. On Wednesday we had two work sessions for our updated C-day deliverables and a meeting on Thursday to discuss the workload for our milestone 3 deliverables. Lastly, we had a meeting at the writing center where we discussed recommendations for our research paper.

Key Events:

Finished Deliverables for milestone 3 and submitted updates for C-day.

Member activities

Team member name	Major tasks and contributions	Workload (hours)
Robin Tandongfor	Worked on milestone 3 presentation PowerPoint slides (red phase). Worked on updating C-day poster. We also had a meeting with the writing center.	10
Jack Pursley	Worked on blue phase PP slides and added the blue team’s contributions to the research paper.	10
Kylah Wilson	Worked on and prepared for milestone 3 presentation, completed part on C-day poster, and added finishing touches to final research paper.	10
Elijah VanDorn	Contributed to blue team’s PowerPoint slides along with milestone challenges Also created 30 sec. video for C-Day presentation. Reviewed our research paper for final turn in.	10
Valentine Wairimu	Collaborated with the team to prepare for Milestone 3 presentation Assisted the team prepare for C day presentation. Helped the team to tweak the poster to a professional standard.	10
	Team Total	

Report Week: 11/03 to 11/10

Status: Green, Yellow, or Red:

Green

Progress summary:

We finalized the red/blue team phase, submitted our C-day poster, and are now working on our milestone deliverables and presentation.

Meeting Summary:

We held three meetings this week on Wednesday, Thursday, and Sunday. In our Wednesday and Thursday meetings we shared our research and progress from both the offense and defense and worked together to combine our reports. We also divided our Millstone Presentation work. On our Sunday meeting we held a work session for our Milestone 3 Presentation.

Key Events:

Submitted poster for C-day. Finalized red/blue team phase.

Member activities

Team member name	Major tasks and contributions	Workload (hours)
Robin Tandongfor	Attempted to exploit vulnerabilities on open ports from stealth scan, transferred research onto PowerPoint presentation.	13
Jack Pursley	Logged another brute force attack from another unknown IP address. They did not know what the admin name was but tried several times. Kept tabs through Logwatch to spot any potential signs of intrusion.	10
Kylah Wilson	I completed a penetration testing project, which included performing a stealth scan to identify vulnerabilities. I then added to the project summary in the presentation.	10
Elijah VanDorn	Conducted red team penetration testing with VPN-assisted scans to bypass firewall blocks and monitored server activities. Supported the blue team by running Logwatch scans for intrusion detection and collaborated with teammates on milestone 3 deliverables.	10
Valentine Wairimu	Participated in penetration testing for red team including but not limited to stealth scan. Assisted to monitor any potential invasion of	10

	any kind to our server. Collaborated with team to guide milestone 3 deliverables.	
	Team Total	53

Report Week: 10/27 to 11/03

Status: Green, Yellow, or Red:

Green

Progress summary:

We are in continuation of the red/blue team phase.

Meeting Summary:

We held three meetings this week on Tuesday, Wednesday, and Thursday which were all work sessions on our red/blue team phase, and we shared the work we have done both on offense and defense.

Key Events:

Continuation of Red/Blue Team Phase.

Member activities

Team member name	Major tasks and contributions	Workload (hours)
Robin Tandongfor	Attempted to exploit vulnerabilities from the stealth scan and documented analysis from attempts.	10
Jack Pursley	Kept tabs on logs dealing with wrong passwords and wrong credentials for defense on our server. No signs of scans or suspicious use of sudo. Disabled attackers' ability to run some commands without passwords when using Visudo.	11
Kylah Wilson	Researched penetration testing, passwords, and access control. Attempted to identify potential vulnerabilities in the server	10
Elijah VanDorn	Ran scans on the opposing team’s server with a VPN since initial IP got stopped by the firewall after the first time running a scan. Found some open ports; continuing to research potential vulnerabilities within those (ports) to expose.	10
Valentine Wairimu	Red team participation (Offense team) Performing stealth test for our target IP address to test any security vulnerabilities. Documented the analysis of any open ports and offered recommendations on security	9

	measures that would ensure more security.	
	Team Total	50

Report Week: 10/20 to 10/27

Status: Green, Yellow, or Red:

Green

Progress summary:

We reviewed the red team/ blue team phase and what was expected according to our project plan. We split the team into two groups where one team focuses more on offense while the other is more focused on defense.

Meeting Summary:

We held 3 meetings this week on Tuesday, Thursday, and Friday. Where we discussed the red/blue team phase, had a work session where we researched penetration/defensive tools, and performed a stealth scan.

Key Events:

We received our target IP address initiating the beginning of the RED/BLUE Team phase:

Member activities

Team member name	**Major tasks and contributions**	**Workload (hours)**
Robin Tandongfor	Research Penetration tools (Nmap. Metasploit) and stealth scanning commands (i.e TCP SYN Scan). Perform stealth scan using Nmap and spent some time researching how to perform these commands without being detected and put it in the Penetration Testing Help Doc.	9
Jack Pursley	Pen-tested with Nmap on our IP address. Got level 250 “good luck” with TCP sequence prediction. It also Couldn’t determine OS. Did find the open ports, though. Installed rkhunter to scan for potential rootkit malware. Updated RHEL 8 again, correctly enabled fail2ban jails. User tried to get in using Administrator and root names, didn’t get in, but was briefly able to disable firewalld.	10
Kylah Wilson	Researched Penetration and security tools. Discussed with group on ways to prepare for the red/blue team exercise.	10

Elijah VanDorn	Tasked with monitoring server logs and identifying any anomalies or potential breaches as part of the defense team. Collaborated with Jack to review logs in real-time. Contributed to identifying weak points for fortifying the server against future threats.	10
Valentine Wairimu	Participated in team penetration testing to identify threats within our system. Conducting Stealth scan to intrude the provided system to test their defenses and weaknesses	10
	Team Total	49

Report Week: 10/13 to 10/20

Status: Green, Yellow, or Red:

Green

Progress summary

This week, we completed our deliverables for the Information Security Policy and Risk Mitigation phase. Then, we worked on creating content for the milestone 2 presentation. We presented on Thursday, October 17 and then focused on submitting and updating our Milestone 2 deliverables required for our report, such as the updated Gantt chart, updated Project Plan, updated Research Paper, and implemented the feedback from the previous milestone.

Meeting Summary:

We had four meetings this week, including our Milestone Presentation. Our first meeting took place on October 16, and it was a rehearsal for our Milestone Presentation. We had another meeting at 8:30 pm the same day, which was also a rehearsal. Our third meeting was another rehearsal on October 17, and then we had our Milestone Presentation at 4:30 pm that day.

Key Events:

We had our milestone report presentation on October 17 and submitted our milestone deliverables on October 20.

Member activities

Team member name	**Major tasks and contributions**	**Workload (hours)**
Robin Tandongfor	Updated Gantt Chart and Research Overview. Created slides for security Policy and deliverables, updated gantt chart, updated resource overview and Milestone 3 preview in our presentation. Rehearsed presentations and added 3 policies under the security policy	15

	in the “Project Outcomes and Achievements Summary” section.	
Jack Pursley	Created the YouTube video to put in the comment section of Milestone 2. I Rehearsed the presentation along with everyone else three times. Added my part of the research paper in for draft 2 under “Project Outcomes and Achievements Summary”.	13
Kylah Wilson	Rehearsed and prepared for presentations, completed my part in the research paper draft, and completed more research for the Security Policy.	12.5
Elijah VanDorn	Worked on the Access Management Policy for Milestone 2, ensuring that user roles, permissions, and security controls were clearly defined. Assisted in the presentation rehearsal to ensure smooth delivery for the Milestone 2 presentation. Provided support in updating the Research Paper, focusing on integrating security policies and risk mitigation strategies. Participated in team meetings to refine deliverables and ensure alignment with project goals.	13
Valentine Wairimu	Worked on research on Security Policy and Risk Assessment and management. Participated in the presentation for the Milestone 2 risk assessment, Updated the Project plan – Objectives, Background overview and QA plan. Assisted the team in organizing the work for Milestone 2	10
	Team Total	63.5

Report Week: 10/7 to 10/13

Status: Green, Yellow, or Red:

Green

Progress summary

Finishing touches have been added to our security policies and assessments to be added to our second draft of the research paper. Additional bugs have been patched in our server as well.

Meeting Summary

We had our three recurring meetings on Tuesday, Wednesday and Thursday, where we discussed each other's progress. Robin and Kylah discussed their work on their policies, while Jack and Valentine discussed their findings on the server itself. Elijah has been working on his risk assessment as well.

Key Events:

A problem with a password configuration caused us to be denied access to the server, but Josh Garske was able to undo it. We also asked him to create a snapshot of our server in case the VM goes down again, which he did.

Member activities

Team member name	Major tasks and contributions	Workload (hours)
Robin Tandongfor	Worked on enabling plugins in the Maria DB. Wrapped up security policy. created template for milestone 2.	10.5
Jack Pursley	I Downloaded Aide, an open-source file integrity monitoring tool used to detect unauthorized file modifications. I Installed rng-tools, a package that helps bridge the HW RNG and the kernel's entropy pool. I Enabled automated system updates with dnf-automatic. I Enabled the rsyslog service. Finally changed the server admin root password. For Apache, I added various security headers, such as disabling MIME sniffing, enabling XSS protection, bug squashing to prevent clickjacking, enabling HSTS, and setting content security policy.	14
Kylah Wilson	Continued working on security policy research and prepared for upcoming presentations	10
Elijah VanDorn	Finished the access control portion of policy, analyzed insights on risk exposure, evaluated potential vulnerabilities related to the patched bugs.	9.5
Valentine Wairimu	Continued Milestone 2 research on security policies and worked with Jack to identify Risk mitigations on challenges that the team has faced throughout the project. Documented these risks alongside the desired mitigations.	10

	Researching on trying different methods of saving work in local files in case VM crashes. Assisted to document this and practice on the best method which will be decided by Jack and I on our next meeting tomorrow.	
	Team Total	44

****

Report Week: 9/30 to 10/6

Status: Green, Yellow, or Red:

Green

Progress summary

Tasks were distributed between members, and we updated the Gantt chart to improve our time usage. The team has been doing individual research on upcoming

Meeting Summary

The team meets on Tuesday, Wednesday and Thursday as we did this past week. The team continued collaboration on the upcoming tasks regarding Information Security Policy & Risk Mitigation. We discussed success and challenges that we may be facing during our project research and agreed to continue doing research on the topic. Each team member is playing a different role in the research as we have split up the work and as we get closer to the due date, we will review the work together. We also discussed the feedback that we received from our weekly reports and milestone 1.

Key Events:

We held meetings six through eight this week.

Member activities

Team member name	Major tasks and contributions	Workload (hours)
Robin Tandongfor	Continued research for Information Security Policy & Access Control. Updated Project Plan.	10
Jack Pursley	Updated RedHat server (again), Downloaded ClamAV malware scanner (again), confirmed manually that GRUB2 works correctly, downloaded Bind DNS software, and confirmed DNSSEC is working correctly.	13
Kylah Wilson	Research on Information Security Policy & Access Control	10
Elijah VanDorn	Continued research on Information Security Policy & Access Control, with a focus on gathering and synthesizing data that will support our project's final phase.	11

Valentine Wairimu	Continued research on Information Security Policy and Access Control and gathering necessary information for final work.	9
	Team Total	55

****

Report Week: 9/23 to 9/29

Status: Green, Yellow, or Red:

Yellow

Progress summary

Tasks for phase two were distributed between members, and we updated the Gantt chart to improve our time usage. The team has been doing individual research.

Meeting Summary

This week, we had two meetings on Tuesday and Wednesday. During our Tuesday meeting, we discussed allocating responsibilities for the Information Security Policy & Risk Mitigation phase. In the second meeting, we reviewed and updated the Gantt chart to improve our project timeline by setting earlier deadlines. A third meeting was planned, but some of us encountered service outages. We also encountered a server outage issue, prompting us to focus on research activities while we wait to hear back from Josh Garske.

Key Events:

The fourth and fifth weekly meetings took place on Tuesday and Wednesday.

Member activities

Team member name	**Major tasks and contributions**	**Workload (hours)**
Robin Tandongfor	Created a template and began working on the Information Security Policy & Access Control. Updated Gantt chart.	9
Jack Pursley	Updated RedHat and its Kernel packages. Disabled reveal PHP. Successfully corrected some key pair matching within Kernel hardening before the server went out.	10
Kylah Wilson	Research for Information Security & Access Control	10
Elijah VanDorn	Begin working on and researching policy on access control including starting to work on draft	10
Valentine Wairimu	Began research on Information Security Policy and Access Control	10

	Team Total	49

****

Report Week: 9/16 to 9/22

Status: Green, Yellow, or Red:

Green

Progress summary

The team has progressed on finalizing the Risk Assessment Phase. Key vulnerabilities have been identified, and common threats to the website infrastructure have been documented. The risk assessment document is nearing completion, with the team collaborating on compiling recommendations for risk mitigation.

Meeting Summary

The weekly meeting focused on reviewing the progress of the risk assessment and the upcoming deliverables for Milestone 1. Team members discussed findings from research and collaborated on drafting the report. Each member was tasked with a relevant section of the research paper according to their assignment in the project plan.

Key Events

- The team is in the final stages of compiling the risk assessment document for submission.
- Key threats and vulnerabilities have been documented, and the team is preparing to transition into the next phase of the project

Member activities

Team member name	Major tasks and contributions	Workload (hours)
Robin Tandongfor	Got the Ecommerce sites live. Part 6 a and b of the report have been written. Documented and researched critical assets. Did “critical assets” and “Gantt chart” portion of Milestone 1 presentation. Updated Gantt Chart and WBS. Downloaded and ran some vulnerability tools.	12
Jack Pursley	Continued analysis of our server infrastructure. Part 5b of the report has been written, specifying the overall technical state of our server. Created the first parts of the PowerPoint and Research Paper.	12
Kylah Wilson	Parts 1-4 on the Report, Network Defense Plan, Research fl	10
Elijah VanDorn	Conducted in-depth research on risk assessment: Focused on analyzing critical	8

	assets of the website infrastructure and their vulnerabilities. Analyzed common threats: Evaluated potential security risks, including malware, DoS attacks, and unauthorized access.	
Valentine Wairimu	Project Outcomes and Achievements of Research paper draft, Identified Milestone 1 challenges and participated in presenting, Updating Project plan.	9
	Team Total	51

****

Report Week: 9/9 to 9/15

Status: Green, Yellow, or Red:

Yellow

Progress summary

We have set up both the VM and the server. Additionally, we have conducted research on the Red Hat Linux server, the software installed on the server, and their common vulnerabilities, along with vulnerability assessment tools. Work has been done to get the website activated and get our VMware IP address active in Apache. We are currently in the yellow since we are still trying to get the website working and our presentation fully ready.

Meeting summary

In meeting 3, we worked together trying to make ecommerce site live and shared research such as vulnerability tools.

Key events

The third weekly meeting took place on Wednesday the 11th. We have set up and gotten familiar with the VM and the server.

Member activities

Team member name	Major tasks and contributions	Workload (hours)
Robin Tandongfor	Set up VM and server. Researched red hat Linux server. Researched pre-installed software's on the server and their common vulnerabilities. Researched vulnerability tools. Installed vulnerability tools or scans like Nmap.	11
Jack Pursley	Edited Apache in command line to be updated to our IP address. Edited Word Press in command line to try and get it up and running. Researched terminal prompts for navigation in Apache, MariaDB, and RedHat.	9

Kylah Wilson	Researched possible threats and network defense plans.	5
Elijah VanDorn	Analyzed prominent defense structures that best fit our project; gathering ideas and concepts to incorporate.	4.5
Valentine Wairimu	Setting up VM and Server, researching on ways that the team could find useful methods in exploring and curving security vulnerabilities.	5
	Team Total	34.5

****

Report Week: 9/1 to 9/8

Status: Green, Yellow, or Red

Green

Progress summary

The Project plan has been completed and we are now getting ready for phase 1. During the development of our RACI chart, we created a few group roles and determined who would be Responsible, Accountable, Consulted, and Informed.

Meeting summary

In meeting 1, we went over assigned tasks, communications agreement, and reviewed the RACI and GANTT charts for the Project Plan. In meeting 2, we went over our contributions and workload in preparation for Phase 1.

Key events

The first weekly meeting was on August 30. Project Plan was submitted September 1st. The second weekly meeting was on September 4th.

Member activities

Team member name	**Major tasks and contributions**	**Workload (hours)**
Robin Tandongfor	Made edits to project plan/GANTT chart	6
Jack Pursley	Made edits to Project Plan/Future Meetings and Collaboration plan.	5
Kylah Wilson	Made edits to project plan/RACI chart	4
Elijah VanDorn	Researched information regarding RACI chart	3
Valentine Wairimu	Collaboration with InComm Payments project team	5
	Team Total	23