Ira A. Fulton Schools of Engineering
Arizona State University

CSE 545: Software Security

PCTF Project Proposal

Team Name

Team0xC

Team Members

- Joshua Gomez, joshuago78@gmail.com
- Jonathan Chang, jachang3@asu.edu
- Michael Kotovsky, michael.kotovsky@intel.com
- Jonathan Ong, jong16@asu.edu
- Kumar Raj, kraj6@asu.edu
- Mehran Tajbakhsh, mehrantajbakhsh@gmail.com

Project Goal

What is the goal of your project?

To automate the discovery of attacks against us and the execution of attacks against our opponents.

Project Idea

What would your team like to do for the project?

CLAMP: CTF Logger Analyzer Mimicker Patcher

Database
We will use an existing tool, such as a SQLite3, to perform this function

- Keeps track of two related concepts: vulnerabilities and exploits
- Vulnerabilities are recorded sequences of requests and responses that resulted in one of our services losing a flag
- Vulnerabilities can be marked as: open, benign (flag retrieved by game admin), weaponized, and patched
- Exploits are attack scripts that will be run against our opponents
- Exploits record number of flags captured in previous rounds and also keep a cumulative total

Script 0: Executor

This script is the orchestrator of our attacks and will be custom built by our team

- Uses a database of exploit scripts
- Automatically executes exploit scripts against all opponents every round
- Automatically submits captured flags
- Records which exploits resulted in captured flags
- In successive rounds the exploits are sorted and run in the order of decreasing performance in the previous round (i.e. scripts that actually captured flags are run first)
- New exploits can be added to the database at any time and are run first on the next round

Script 1: Logger

We will use an existing tool, such as Nginx or HAProxy, to perform this function

- Logs all requests from masquerade IP to our server
- Logs all responses from our server to the masquerade IP

Script 2: Analyzer

This will be a custom script built by our team

- Analyzes logs produced by Logger
- Looks for responses containing flags
- Finds request(s) that resulted in that response
- Compares sequence of requests and responses to known vulnerabilities in the database
- If the sequence is novel, the Analyzer adds the sequence of requests and responses as a new vulnerability in the database

Script 3: Mimicker

This could be a custom script built by our team. However, it will be very difficult to automate in just 3 weeks. Therefore, this will likely end up being a manual process performed by team members during the live event.

- Looks for new vulnerabilities in the database
- Generates a new exploit script based on the series of requests and responses
- Adds the exploit to the database
- Updates the vulnerability as being weaponized

Script 4: Patcher (human in the loop)

This would be impossible to automate in the given time frame. Therefore, this will be a manual operation performed by team members during the live event.

- Prior to the competition the team will put together 2 checklists:
    - Checklist 1: Server prep
        - A list of actions to take in the hour before the game begins
        - These will harden our server as best we can
    - Checklist 2: Service patching
        - A list of common vulnerabilities to look for along with the recommend actions to patch them
- Team member looks at new vulnerabilities in the database
- Team member determines if the recorded vulnerability was really an attack or a legitimate retrieval of the flag by the game admin
- If it was legit, Team member updates the vulnerability in the database as benign

- If it is a vulnerability, the Team member consults the checklist and determines the best way to patch it
- Team member patches the service
- Team member updates the vulnerability in the database as being patched

Team Member Contributions

How has each team member contributed to the overall project idea?

- Joshua Gomez: attended group brainstorming meeting, participated in Slack discussions, drafted proposal
- Jonathan Chang: attended group brainstorming meeting, participated in Slack discussions
- Michael Kotovsky: attended group brainstorming meeting, participated in Slack discussions
- Jonathan Ong: attended group brainstorming meeting, participated in Slack discussions
- Kumar Raj: attended group brainstorming meeting, participated in Slack discussions
- Mehran Tajbakhsh: attended group brainstorming meeting, participated in Slack discussions

Plan and Timeline

What is your team's drafted plan and timeline to complete the project?

Course High-Level Timeline for Planning

- *Week 2: Recommended virtual meeting with course team member*
- Week 3: PCTF Project Proposal due
    - *Recommended virtual meeting with course team member*
- Week 4: PCTF Status Update due
    - *Recommended virtual meeting with course team member*
- *Week 5: Recommended virtual meeting with course team member*
- Week 6: PCTF Game Play
- Week 7: PCTF Final Report due

Due Date	Responsible Party(ies)	Action Item
1/30/22	Joshua Gomez	Project coordination • Draft proposal • Set up Github repo
2/1/22	Joshua Gomez	Database • Document schema

		• Setup ORM models
2/4/22	Michael Kotovsky & others	Logger • Select tool • Document configuration • Write filter scripts (if needed)
2/4/22	Jonathan Ong & others	Patcher • Draft Checklists
2/7/22	Jonathan Chang & others	Executor • Complete basic functionality
2/11/22	Mehran Tajbakhsh Kumar Raj & others	Analyzer • Complete basic functionality

Course Team Questions

What questions do you have for the course team?

1. On Adam Doupé's website he has a syllabus from a past instance of this course. On it he has recommended project ideas. These are all exploitation and defense tools. Our proposal is more of a CTF gameplay tool. Is this sufficient?

References

What resources and reference materials have you used to support your team's project idea? Use IEEE format (formatting reference: Owl Purdue: IEEE Style > Reference List].

R. Mukherjee. "CISCO SECCON AD-CTF 2020". Medium. https://medium.com/csictf/cisco-seccon-2020-ad-ctf-2614b27f387a (accessed January 16, 2022).

A. Doupé. "Software Security - S16". adamdoupe.com. https://adamdoupe.com/teaching/classes/cse545-software-security-s16/projects.html (accessed January 24, 2020).

Submission Directions for Project Deliverables

Your team's PCTF Project Proposal must be a single PDF or Word doc with the correct naming convention: Your Team Name_PCTF_Project Proposal.

You *must* submit your team's PCTF Project Proposal in the designated submission space in the course. Learners may **not** email or use other means to submit the project for course team review and feedback.