Ira A. Fulton Schools of Engineering
Arizona State University

Engineering | School of Computing, Informatics, and Decision Systems Engineering

CSE 545: Software Security

PCTF Status Update

Team Name

Bindevil

Team Members

- Captain: Vo Minh Duy, vduy1@asu.edu
- Kosuke Nagae, knagae@asu.edu
- Hongbo Wu, hongbowu@asu.edu
- He Jiang, hjiang81@asu.edu
- Jinyi Yu, jinyiyu@asu.edu

Project Goal

What is the goal of your project?

There are two main goals in our project:

1. Defend our services against other teams' attacks, protect our flags from being captured by finding vulnerabilities in our system and patching our services.
2. Analyze other teams' services, find and exploit the vulnerability of other teams' systems, and try to access their server to capture the flags.

Accomplishments and Contributions

What has been accomplished so far and how has each team member contributed?

- All members: the binary hacking and web hacking assignment provide important knowledge about CTF game; we are trying to complete the learning materials and the assignments as soon as possible to gain practical experience prepare for the game.
- Vo Minh Duy: write PCTF Proposal and PCTF Status Update. He has completed week five learning materials and is working on binary hacking assignment level 5. Besides the course assignment, he is also doing Toddler's Bottle wargame on pwnable.kr and watching Professor Adam Doupé walkthrough video of the wargame. Furthermore, he is

in charge of network attack techniques: sniffing, scanning, IP/UDP/TCP spoofing, hijacking, and plans to develop an automatic tool for scanning the network periodically. The tool development has not started yet.

- Hongbo Wu: focus on researching SQL injection, CSRF, and XSS attacks. He has provided the team with a summary about the topic and the usage of SQLMap, which he plans to use for SQL injection attack.
- Kosuke Nagae: research on application vulnerability, especially file access and command injection. He has completed the binary hacking assignment to build up knowledge and experiences in this topic.
- He Jiang: he is in charge of command injection and string-format vulnerability. He has completed the binary hacking assignment and is focusing on the web hacking assignment.
- Jinyi Yu is currently at level four of both binary and web hacking assignments. He is trying various previous CTF games on the online source to well prepare for the game.

Updated Plan and Timeline

What are the remaining project needs and deliverables and who are the responsible team members for these?

- All team members:
  - Learn more materials (watching videos, reading, participating in online wargame…) about the CTF challenge, share useful resource across the teams.
  - Complete the learning material and binary/web hacking assignment to prepare knowledge and experiences for the game.
  - Practice using exploitation tools like ghidra, gdb, pwntools…
- Vo Minh Duy: Write automatic network scan script.
- Kosuke Nagae: Learn how to use Metasploit. Build some scripts for Metasploit that automatically scans vulnerability
- Hongbo Wu: more research on using SQLMap

Course High-Level Timeline for Planning

- 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
Feb 11th	Kosuke Nagae	Learn how to use Metasploit
Feb 11th	Vo Minh Duy	Write automatic network scan script

Feb 14th	All members	Search CTF resources and useful tools of both defensive and offensive sides. Each member researches more profound about own topic.
Feb 17th	All members	Team meeting, sharing discovered information or knowledge in the team. Use and test selft written script/researched tools to get familiar before the game. Complete CTF game preparation: confirm each member's schedule and role, ensure the whole team know about tools that plan to use during the game
Feb 18th	All members	Participate in PCTF game.

Course Team Questions

What questions do you have for the course team?

References

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

[1] OffSec Services Limited. "METASPLOIT UNLEASHED – FREE ETHICAL HACKING COURSE". Offensive-security. https://www.offensive-security.com/metasploit-unleashed

[2] Rapid7. Metasploit Documentation. Rapid7. https://docs.rapid7.com/metasploit/

[3] Rohit Dhamankar et al. Sans top-20 security risks, 2007. SANS. http://www.sans.org/top20/2007/

[4] Barth, Jackson, Mitchell. Robust Defenses for Cross-Site Request Forgery, 2008

[5] Rejah Rehim, Python Penetration Testing Cookbook, 1st ed: Packt Publishing, 2017.

[6] daehee "PWNABLE.KR". Pwnable.kr. https://pwnable.kr/index.php

[7] Adam Doupé "Walkthrough on Pwnable.kr". Youtube. https://www.youtube.com/playlist?list=PLK06XT3hFPziMAZj8QuoqC8iVaEbrlZWh

Submission Directions for Project Deliverables

Your team’s PCTF Status Update must be a single PDF or Word doc with the correct naming convention: Your Team Name_PCTF_Status Update.

You *must* submit your team’s PCTF Status Update in the designated submission space in the course. Students may **not** email or use other means to submit the project for course team review and feedback.