Ira A. Fulton Schools of Engineering
Arizona State University

CSE 545: Software Security

PCTF Project Proposal

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.

Project Idea

What would your team like to do for the project?

At first, we plan to complete the course materials and assignments as soon as possible since these works provide much knowledge and experience for the PCTF challenge. Furthermore, each team member will be in charge of specific topics/techniques in this project. The team member will focus on researching the chosen topics by reading documents, learning to use open source tools, or building tools to help during the game. When the game begins, each member will use their technique/knowledge to participate in the competition.

Team Member Contributions

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

Although our team splits the work among the members based on the topics, it does not limit that each member only does their part during the game. Moreover, all members will participate in the game together and help each other if they discover vulnerabilities outside their researched topic. Each member is in charge of topics as follow:

- Vo Minh Duy: focus on network techniques like sniffing, scanning, IP/UDP/TCP spoofing, hijacking. Try to gain a deeper understanding of these techniques and develop an automatic tool for scanning the network periodically. The tool may output an analysis text file or write to an online spreadsheet which is shared with all members.
- Kosuke Nagae: focus on application vulnerability, especially file access and command injection. Build some scripts for Metasploit that automatically scans vulnerability. Patch our service and also try to hack opponent's one based on the result of auto-scanning.
- Hongbo Wu: focus on researching SQL injection, CSRF, and XSS attacks. Plan to write a script to make web request with SQL injection, CSRF, and XSS.
- He Jiang: research more profound on command injection (web vulnerability) and string-format vulnerability (binary vulnerability).
- Jinyi Yu: focus on memory corruption exploitation and format-string vulnerabilities. Practice using pwn tools like ida, ghidra, gdb, and try the previous pctf on the online source to well prepare for the game.

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
Feb 7 th	All members	Search CTF resources and useful tools of both defensive and offensive sides. Each member researchs more profound about own topic.
Feb 7th	Kosuke Nagae	Learn how to use Metasploit

Feb 7th	Vo Minh Duy	Write automatic network scan script, try integrating wireshark, scrapy in python for packet analysis
Feb 7th	Hongbo Wu	Write script to make web request
Feb 14th	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?

1. What does "the script bot" do other than putting flags on each team's server? How does it interact with the service? Can we know it before starting the game, or do we need to analyze what is going on at the time of the game?
2. How about the distribution of the flags from different types of vulnerabilities? The percentage of network, application, or web?
3. Can we access the internet from the team's server for tool installation?

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].

[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.

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.