**PCTF Status Update**

**Team Name**

JSY-ACE

**Team Members**

* Afshin Paydar, [apaydar@asu.edu](mailto:apaydar@asu.edu) (Captain)
* Chao Wan, [cwan13@asu.edu](mailto:cwan13@asu.edu)
* Edy Widjaja, [ewidjaja@asu.edu](mailto:ewidjaja@asu.edu)
* Jie Jin, [jjin19@asu.edu](mailto:jjin19@asu.edu)
* Santoso Ham, [sham8@asu.edu](mailto:sham8@asu.edu)
* Yan Xue, [yxue36@asu.edu](mailto:yxue36@asu.edu)

**Project Goal**

**What is the goal of your project?**

1) Defend our system against attacks, protect our flags from being captured by ensuring confidentiality and integrity, and at the same time maintain the system’s availability.

2) Try to break into other machines and develop exploits in order to capture the flags as many as possible.

**Accomplishments and Contributions**

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

* All members: Search CTF resources and useful tools of both defensive and offensive sides, collect penetration techniques which can be used to obtain privileged access to other machines
* Santoso: ideas for defend side - a) LAN: write scapy code to listen all traffic in the LAN, b) OS: may need hardening of the OS and create a bash shell to patch / close open ports; c) Router: close the incoming connection such as TELNET or other ports that we don't use, and firewall on the router side to accept connections from port 80/443, don't allow ARP broadcast.
* Edy: ideas for attack side – develop the code to scan/sniff/attack; summarize meeting notes.
* Afshin: we can build a tool to scan the local system with pre-installed services, and detect the built-in security bugs/flaws, try to patch the vulnerabilities. The tool will scan all open ports and static source code for the following type of risks: XSS (Cross-site scripting), SQLi (SQL injection), XXE (XML External Entities), RCE (Remote Code Evaluation), LFI (Local File Inclusion), RFI (Remote File Inclusion). Create a GitHub private repository for project coordination
* Yan: organize meeting, write PCTF-Status-Update

**Updated Plan and Timeline**

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

All team members:

1. learn more materials (watching videos, reading etc.) about the CTF challenge, share useful resource across he teams.
2. Write code for vulnerability scanning, traffic listening etc.

**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 12th | All members | Watch resources, learn and test tools for CTF challenges |
| Feb 12th | All members | Follow up meeting |
| Feb 19th | All members | Complete CTF game preparation: confirm each member’s schedule and role, ensure the whole team know about tools which will be used during the game |
|  |  |  |

**Course Team Questions**

**What questions do you have for the course team?**

1. [Enter Text and delete brackets]
2. [Enter Text and delete brackets]
3. [Enter Text and delete brackets]
4. [Enter Text and delete brackets]
5. [Enter Text and delete brackets and adjust the number of questions to suit the team’s needs]

**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](https://owl.purdue.edu/owl/research_and_citation/ieee_style/reference_list.html)].

[1] Mohit, *Python Penetration Testing Essentials*, 1st ed: Packt Publishing, 2015.

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

**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.