**PCTF Project Proposal**

**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.

**Project Idea**

**What would your team like to do for the project?**

To defend the system, we plan to use tools such as ARP spoof detector, web vulnerability scanner, IDS/IPS. As for the attack effort, we are thinking about utilizing reverse engineering tools such as gdb, objdump for binary hacking. Ideally, we hope to build tools to help automate some tasks during the game. Per request, python 3 will be used to communicate with the platform.

**Team Member Contributions**

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

* The ideas came from all members.
* Afshin Paydar: Writing Code/ Read Documentation

**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 7th** | 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 |
| **Feb 14th** | All members | Learn and test the tools above, build automation scripts for potential uses |
| **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. In each machine, will flags be stored in the same place every time?
2. Do we expect to use Ubuntu system during the game?
3. Does the source of all traffic(Game bot & other VMs) are one MAC address in the CTF?

**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](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.

[3] Jose Manuel Ortega, Mastering Python for Networking and Security, Packet Publishing 2018

[4] Marcus Pinto; Dafydd Stuttard, The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws, Publisher: Wiley 2007

**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. Students may **not** email or use other means to submit the project for course team review and feedback.