Introduction to Security

Luis Garcia
USC CSCI 430

CTF 1 Overview
CTF1 Overview: Secure Server

• We’re going to practice setting up and monitoring a web server
• Each team will play the defender role (Blue team) for their own system and the attacker role (Red team) for another team's system.
CTF1 Overview: Secure Server

- **Topology:**
  - /proj/USC430/CTF_Bank/cctf.ns.

- **Teams can share files by placing them into the /groups/USC430/team_133_x/ folder where "x" should be replaced with the team's number (1-5)**

- **Structure:**
  - Team 1 will defend blue node in their experiment - uscbank1.
  - They will also have access to red node in the experiment of team 2 - uscbank2, and they will launch attacks on blue node in uscbank2 experiment.
  - Team2 protects blue node in uscbank2 and attacks from red node in uscbank3.
  - And so on.
Blue Team Tasks

• This team will control the blue server.
• Goal: Develop several applications so that they function as specified, and to secure them and the network against intrusions.
• The applications to be supported:
  – Web server with a banking application
  – DB server to support the banking application
• The team should also locate and close any unnecessary applications that may be used as a backdoor.
  – I will open a few backdoors at the competition stage and you will need to find them and close them.
Blue Team Tasks:
Web server with a banking application

• Use any web server you’d like (e.g., Apache)
• Should look like this:
  – It is a publicly accessible application
  – When the page blue/register.php?user=A&pass=B is accessed from the red node, the system creates a new account for user A with pass B in the system.
  – When the page blue/login.php?user=A&pass=B is accessed, the system validates the user login and serves the user a cookie.
  – When the page blue/manage.php?action=C&amount=D is accessed, the system performs action C with amount D. Below are the possible combinations of action and amount:
    • action=deposit, amount=D - add amount D to the user's account and display balance
    • action=withdraw, amount=D - withdraw amount D from the user's account if there are sufficient funds and display balance
    • action=balance, no amount variable specified - print out balance from the user's account
    • action=close, no amount variable specified - close out the user's account
  – When the page blue/logout.php is accessed, the user is logged out and the cookie invalidated.
Blue Team Tasks:
Web server with a banking application

- Balance should be displayed in the following format
  - "balance=VALUE"
- You may put any other information on the Web page returned to the user.
- Blue network will receive legitimate user requests from the red node.
  - They will also receive attack traffic from the red node.
  - Red node will use IP aliasing to claim multiple IP addresses.
  - An IP in the red network can be legitimate, attack or both.
  - Red team and my scoring program can create IP addresses in the red network on the fly.
  - My scoring program will further create only legitimate IPs - red team will not be allowed to use these for attacks.
  - **The goal of the blue team is to serve all requests coming from legitimate IPs and to either serve or drop requests coming from the attack IPs.**

Make sure you understand how `iptables` command works before you use it as you may cut off your access to a given machine in DeterLab if you filter out some specific traffic to/from it, e.g., all outgoing traffic. The only way to recover from this is to reboot the machine using Web portal for DeterLab. Click on your Experiment, then click on the machine's name in the Node List (e.g., pc133) and then choose "Reboot node" from the top left menu. It usually takes 5-10 minutes for the machine to come up again.
Blue Team Tasks:
Suggested Division of Work

• 2-3 people work on one server’s development and configuration.
  – Monitoring should also be done on server to ensure that all accesses are logged, and processed correctly.
• 2-3 people should work on monitoring the traffic, detecting and responding to attacks.
  – You can have one person work on finding and closing backdoors.
  – Once you close a backdoor, make sure that it is really closed.
  – make sure you don't close a service that a DeterLab node needs.
  – If you do, you may cut yourself off the network. You will then need to reswap the experiment and try again.
  • DeterLab services are: SSH, inetd, emulab-syncd, pubsubd and ntpd.
Blue Team Tasks: Suggested Strategies

• You may want to limit the ability of attackers to scan your network.
• Make sure to handle SQL injection attacks and to set up folder access conservatively.
• You can set up HTTPS if you like and let me know and I will adjust my legitimate client script to use it.
Red Team Tasks

- This team will control the red node
- I will choose some IPs from the network's range (1.1.1.0/24) to host my legitimate clients and the rest can be used for attacks.
- **Goal:** gain access to blue team's network and interfere with its operation. This can be done by:
  - performing SQL injection
  - making the banking application behave in a way that is not expected (e.g., being able to withdraw money from a legitimate user's account),
  - finding and exploiting a backdoor.
- You can set up a custom IP on redserver like this:
  - `sudo ifconfig ethX:Y 1.1.1.11 up`
  - replace X with the actual interface number for 1.1.1.6 address on red node.
  - Replace Y with a number. Start with 2 and go up with each new address.
- You can use this new address in `wget` or `curl` by doing this: `wget --bind-address=1.1.1.11 URL` or `curl --interface 1.1.1.11 URL`
- You will need to use cookies to access the server. Please explore `wget` and `curl` to learn how to save and use cookies.
Red Team Tasks:  
Suggested Division of Work

• 2-3 people work on different scanning approaches
• 2-3 work on SQL injections
• 2-3 work on sniffing and scanning for backdoors, etc.
Red Team Tasks: 
Suggested Strategies

• Attacking IPs do not have to attack all the time. Mixing up some legitimate traffic with attack would be good to hide the nature of the IPs.
• User passwords/cookies could be sniffed from the net
• It may be possible to leverage an existing vulnerability in OS or applications if you find it.
• Look for backdoors. If they are not closed, you will be able to open a reverse shell into the blue server.
• You can do some hacker training at http://www.overthewire.org or at TryHackMe
Scoring

• The Blue Team receives a point for each legitimate client's request that the server processes and responds to correctly.
• Red Team gets the point otherwise.
Exercise Dynamics

• Teams will need to simultaneously act as Blue Team and Red Team throughout the exercise.
• We will then have a post-mortem discussion and selection of a winning team.
Grading

• Each team member will be graded based on their contribution to the team effort, not based on the team's performance.

• After the exercise each team member will submit a report containing the list of contributions they made to the team effort - e.g., modules that they coded, testing and setup they performed, etc.
  – All team members must sign each report.

• Reports will be delivered to the instructor in class
  – The grades will be assigned based on the report.
Generic Advice for Today until Next Week

1. Define roles and responsibilities
   – Clearly define each team member's roles and responsibilities. Assign tasks based on individual strengths and interests, and ensure that everyone understands what is expected of them.
   – Should expect to work about 1-2 hours per working day

2. Set deadlines
   – Establish clear deadlines for each task or milestone. Make sure they are realistic, and leave some buffer time in case of unexpected delays. Communicate the deadlines clearly to the entire team.

3. Communicate regularly:
   – Establish regular communication channels to keep everyone informed of progress, challenges, and changes. Encourage open and honest communication, and make sure everyone feels comfortable asking questions or raising concerns.

4. Use project management tools:
   – There are many project management tools available that can help teams stay organized and on track. Consider using a tool like Trello, Asana, or Jira to manage tasks, deadlines, and communication.

5. Establish a way to Monitor progress:
   – Regularly review progress against the project plan and adjust as needed. Identify any roadblocks or issues that may be preventing progress and work together as a team to overcome them.
   – Test red team against blue team