2017 ASU Cyber Security Challenge

Challenge Information

Competition Rules

1. All participants must follow ASU ACD 125 policy on Computer, Internet, and Electronic Communications:
   http://www.asu.edu/aad/manuals/policyarchives/ACD/Nov2001/acd125.html
2. Each team can have up to three members.
3. The problems will be released at the beginning of the event.
4. Each team can solve all or part of the competition problems within the duration of the event.
5. The team members are not allowed to discuss the problems with people who are not in their team.
6. All team members are expected to bring their own laptops for connecting to the emulated enterprise network.
7. The team is allowed to download any open-source software packages onto their laptops or servers during the competition.
8. Each team will be graded based on the number of problems the team members have solved. The team with the highest score will be the winning team of the competition.

Networking

Each challenge has its own SSID that will need to be connected to in order access that challenge.

- CyberChallenge-Easy
- CyberChallenge-Medium
- CyberChallenge-Hard

The scoring server will be accessible from any SSID so you can keep track of your score and turn in flags at any time.

- score.cyberchallenge.local

There is only one server for the Easy and Hard challenges.
However, each team will have their own Medium challenge server. Your team number will determine which Medium server you connect to.

- files.cyberchallenge.local
- team##.medium.cyberchallenge.local
- hard.cyberchallenge.local

Scoring Server

Access

To access the scoring server you will need to navigate to the following address:

- score.cyberchallege.local

You will be prompted with the default page where you may either login or register yourself and your team.

Initial Registration

The initial registration should be done by one member of your team. This is because the first member will also be creating the team. After the first account and team are created, then others may be able to sign up, and select their team from the populated dropdown.

Note: This is an insecure and untrusted service. Do not use any accounts or passwords that you normally use. It is against the rules to attack this server or capture any credentials, but be wary.

1. Go to the scoring server address, and then click the "Register" button.
    a.

2. Fill out the presented form with the appropriate information.
    a. Handle: Your account name.
    b. Start a New Team
        i. Team Name: In this section, enter your hacking team name or number.
        ii. Motto: Optional team motto.
    c. Account Password: Your personal account password. Do not reuse real passwords.
    d. Confirm Account Password: Repeat the password you entered previously.
    e. Bank Account Password: The bank will be your total points for captured flags. Make sure you keep this safe. ______________________
3. Click the "Register Account" button.
4. You will get a successful account creation notification. You can now click the Login button to log in, as well as have the rest of your team make their own accounts if needed.

Additional Registrations

Any additional members of your team can create an account and sign up for your team, or you may designate one person as the account manager for your team and have them manage the account and flags.

To sign up additional users, perform the following steps, which are similar to the above.

1. Go to the scoring server address, and then click the "Register" button.
    a.

2. Fill out the presented form with the appropriate information.

   a. Handle: Your account name.
   b. Join a Team
      i. Select a Team: Click on the dropdown and select your team
   c. Account Password: Your personal account password. Do not reuse real passwords.
   d. Confirm Account Password: Repeat the password you entered previously.
   e. Bank Account Password: This feature is not used but is a required field. Enter any password for this and document here. ______________________

3. Click the “Register Account” button.
4. You will get a successful account creation notification. You can now click the Login button to log in, as well as have the rest of your team make their own accounts if needed.

Scoring Server Overview

The scoring server is a service that will be available to all teams so they can enter their captured flags to increase their score and be able to collaborate with team members. The dashboard will show the current status of all teams of flags captured and points scored.

Scoring

The scoring server will track points by distributing money based on captured flags. Flags are weighted differently based on the difficulty and server.

The team with the most money (points) at the end of the challenge will win, and there will be different prizes for the top teams.

When a flag is captured or provided, teams will log into the scoring server and enter the flag into the interface. The server will automatically check the flag and distribute the reward if correct.

Easy Challenge

Access

Join the wifi SSID **CyberChallenge-Easy**. The files for the first Easy challenge can then be found at **files.cyberchallenge.local**
You will be presented with a basic web page with the required files. You can download them however you wish, via web browser or command line with wget or curl.

Cracking Overview

Cracking passwords is an art. Mention of password lists and rainbow tables have been replaced with GPU's and more recently discrete hash cracking machines as the acceptance of cryptocurrency has helped bring about a new age of cracking hashes.

One of your teammates was able to get access to a couple of password hashes from a recent engagement, but needs your help cracking them so he can try to see if those passwords are able to be reused anywhere else in the environment he was in. He was also nice enough to be able to provide an idea of the complexity of the passwords to help you out.
Use a password cracking program like John the Ripper or hashcat to break the hashes and figure out the passwords. The plaintext passwords will be the flags.

Easy Crack 1: Easy1.txt – MD5 5 characters, alphabetic, all lowercase	Easy Flag 1:
Easy Crack 2: Easy2.txt – SHA1 6 characters, numeric	Easy Flag 2:
Easy Crack 3: Easy3.txt – Windows LM 13 characters, alphanumeric	Easy Flag 3:

Your teammate was able to also find an encrypted file on a box he hacked into. Can you help him crack the password protection and look at the contents? A tool such as John the Ripper or fcrackzip may be helpful. The flag will be the password used to open the file.

Easy Crack 4: protected.zip 8 characters, alphabetic, all lowercase	Easy Flag 4:

Packet Inspection Overview

Analysis of packet captures (pcap files) are sometimes necessary for analysts to investigate suspicious activity that may be occurring. You quickly learn why secure protocols are a necessity when doing anything online as cleartext messages can be easily reviewed if they are somehow captured.

Your company’s network team has captured an email transmission from an intruder that was in your building and they have reason to believe they are working with someone else. The individual may have breached your company and is possibly travelling to meet up with their accomplice. It’s up to you to find out some information about them that can be turned over to the proper authorities so they can investigate.
Open the packet capture file with wireshark and follow the streams to find the necessary information. The answer to each question will be the flag.

Easy PCAP 1: What is the intruder’s email address?	Easy Flag 5:
Easy PCAP 2: What is the intruder’s password?	Easy Flag 6:
Easy PCAP 3: What is the accomplices email address?	Easy Flag 7:
Easy PCAP 4: What is the name of the file the intruder sent to their accomplice?	Easy Flag 8:

Medium Challenge

Access

Join wifi SSID **CyberChallenge-Medium**
Then access your team server at **team##.medium.cyberchallenge.local** with browser.

Overview

Welcome to the Medium challenge! For this challenge you will be working through a vulnerable web app: *SwiftImage*. *SwiftImage* is programmed to have vulnerabilities that are representative of vulnerabilities found in the wild and reported in *OWASPs Top 10*.

> ** There are additional vulnerabilities not indexed by our guide, if you find and exploit these vulnerabilities tell a member of the Terra Verde team.

Scoring

Follow the instructions for each exploit that is to be run against the web app. When you successfully exploit the vulnerability, call over a challenge helper from Terra Verde and we will review the results. If they are determined to be successful, you will be provided with the flag that can be entered into the scoring server.

Publicly Accessible Vulnerabilities

These vulnerabilities be exploited without logging in.

Title: **Cross-site Scripting (XSS) -- Reflected**
Goal: Using JavaScript, have a string reflect to the user displaying an alert message or popup.
Description: This vulnerability is located on the HOME page. Certain parameters are not sanitized before being echoed to the user.

Flag 1:

Title: **Parameter Tampering**
Goal: Without a valid user account, find **4** users already registered with *SwiftImage.*
Description: This vulnerability is located on the SAMPLE USER page. How does this webpage process the request to view the sample user? Can we manipulate this parameter to view the other users?

Flag 2:

Title: **Cross-site Scripting (XSS) -- Stored**
Goal: Have a stored JavaScript string reflect to every user that visits the website.
Description: This vulnerability is located on the GUESTBOOK page. All content on this page is stored in the database. One of the fields is not properly escaped causing for malicious code, or not, to be executed on each visit.

Flag 3:

Title: **SQL Injection (SQLi)**
Goal: Log in as an already registered user.
Description: On the GUESTBOOK page there is a registered user that has made a comment about the site. Craft a SQL query for input on the LOGIN page and get access to that users account

Flag 4:

Title: **Command Injection**
Goal: Escape the command being executed to check your password and put the contents of an interesting file, that you should NOT have access to, in the /uploads directory.
Description: On the HOME page follow the link to "create an account", from there, check the strength of your password. Can we escape the grep command being executed and execute our own commands?

Flag 5:

Title: **Remote File Inclusion**
Goal: Load content from a site that you (the hacker) maintain.
Description: On the bottom of every page there is a link to the ADMIN page, following this link will bring you to the next vulnerability. Look at how the request is made for this page it will aid you in loading your content from your site.

Flag 6:

Privately Accessible Vulnerabilities

These vulnerabilities be exploited after logging into the web application.

Title: **Logic Flaw**
Goal: Purchase a photo without using any Tradebux.
Description: There is a photo that you've really wanted to purchase and *SwiftImage* has just sent you a coupon. Using the code **SUPERYOU21** can you get that image?

Flag 7:

Title: **Cross-site Scripting (XSS) -- Reflected**
Goal: Using JavaScript, have a string reflect to the user displaying an alert message or popup.
Description: This vulnerability is located on the user's HOME page in the. Certain parameters are not sanitized before being echoed to the user.

Flag 8:

Hard Challenge

Access

Join the hard wifi SSID: **CyberChallenge-Hard**
Then access server at **hard.cyberchallenge.local**

Overview

This is NOT a boot2root challenge; gather the flags and move on.
Explore every avenue as no hints will be given.
Don't forget to submit your flags to the scoring engine.
Have fun and happy hacking!

Goal

Capture the 5 flags on this box.
They are in the following format: flag{}
The flag itself is the string within the brackets.
Some flags are located in a file named flag.txt

Hard Flag 1:
Hard Flag 2:
Hard Flag 3:
Hard Flag 4:
Hard Flag 5: