642.6
Capture the Flag

SEC642.6

Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

SANS

Capture the Flag

Welcome to Day 6!

Course Roadmap

- Day 1: Advanced Attacks
- Day 2: Web Frameworks
- Day 3: Web Cryptography
- Day 4: Alternative Web Interfaces
- Day 5: WAFs and Filter Bypass
- **Day 6: Capture the Flag**

Network Setup
Exercise Goals
Scope of Work
Rules of Engagement
Start CTF
Four Hours of Game Play
CTF Wrap-Up

This page intentionally left blank.

VPN LAB SETUP

If you use the VPN to connect to the lab, go to Your Labs at

https://connect.labs.sans.org

- Instructions to install and configure OpenVPN to access the lab
- Passwords and certificates required to authenticate
- If you encounter any problems, email virtual-labs-support@sans.org

The VPN lab servers reboot periodically

If you take this class remotely, you need to connect via VPN for the exercises.

Remote students include Mentor, self-study, vLive, Simulcast, community, and OnDemand formats. To connect to the lab environment, SANS makes use of OpenVPN software, which can be installed in Windows, *BSD, Linux, and Mac OS X. The instructions also include certificates and passwords as well as the configuration files for the software to authenticate and connect.

Detailed instructions for the VPN installation are at the following URL:

https://connect.labs.sans.org

After you connect to the VPN, you can perform the exercises for the class. All the exercises require VPN connectivity.

NETWORK SETUP

Connect to the CTF network:

- Live classrooms use the same connection as the rest of the week
- OnDemand and Simulcast attendees create a VPN to the CTF Network, not the Lab Network

Verify network connectivity:

- Pinging 10.42.6.2
- Surfing to score.sec642.org (don't register yet)

Please do not communicate with any other IPs or hostnames yet!

This page intentionally left blank.

DAY 6 GOALS

We apply the techniques we have learned this week

Instead of one at a time, we use the tools and ideas in combination

This is a fun and educational game:

- Some vulnerabilities are modeled after real penetration tests

You can play to win

You can play for fun

You can play to learn and reinforce the exercises from the week

The three are not mutually exclusive!

Today's goals are to work through our methodology in a full web application pen test. Instead of approaching each item or idea separately as we have this week, we approach them as part of a complete test. This enables us to understand how this all works within a typical, or not so typical, penetration test.

Although the test we perform is an example, some are based on real vulnerabilities and applications in the real world. This example was designed to fit within a single day, which does mean that some of it has to be contrived.

Most important goal: Have fun!

ORGANIZATION OF TODAY

Discuss the rules and scope of the game

Your team can then start the penetration test

Play for approximately four hours, hard stop at 14:00

- Breaks are as-needed and not scheduled
- The first team that finds all the flags wins
- Or the team with the most flags at 14:00 wins

After the CTF is over, we will do a debrief, showing where to find all the remaining flags

Today is broken into three parts. The first is this lecture, which sets up the test and explains your scope. The second part is your team performing the test. Early this afternoon, we wrap up the testing. In the last part, we debrief through the application test. You present some of your findings to the instructor and then the instructor walks through anything that was missed and explains the entire test.

TEAMS

Work in teams of 2-5 people

Each team member must record their own findings and notes

The team maintains a master list of flags found:

- Where the flag was found
- How you got to the flag

Have regular meetings every 20–30 minutes:

- Review what you have found
- Compare notes and swap targets
- Adjust and plan your next steps

The game is based on the lab exercises throughout the week

Work in teams, as we recommend that you do in your regular testing. This enables you to combine skill sets and viewpoints to better assess the test. We recommend at least two people and no more than four. More than four becomes overkill in this environment. People start getting left out.

Have all team members record their findings and steps. After class, these notes can be useful for review.

Make sure you have regular meetings to compare notes and make sure you work together. This is extremely important; too often we see people on a team who have pieces of what is needed, but they don't talk to each other.

PROJECT SCOPE

Social engineering is allowed, but the targets are EXTREMELY aware:

- Users may surf URLs you inject

Scope: All web applications on 10.42.6.2-253 (port 80 and 8080)

- Only web applications and web services are in-scope
- Do not attack other services (SSH, DHCP, ARP, DNS, and so on)

Some servers may be accessible only from other servers

642 Inc. operates a DNS server at 10.42.6.2

- You can use this DNS server
- When the exercise begins, try a zone transfer (which isn't an attack)

To determine the risk level of having this information disclosed, 642 Inc. requested a test of all its web applications. This includes all of the web applications in scope. Social engineering is allowed, but the target is security-conscious and aware of the ongoing test. However, any URLs or injected code may be browsed.

Any web application in the network range of 10.42.6.2-253 is within scope of this test. Non-web app services are not. There is a DNS server at 10.42.6.2. This is both the DNS server 642 Inc. uses and the one you should use for the test.

RULES OF ENGAGEMENT

No denial-of-service attacks

No "dangerous" attacks:

- Deleting files or data is not allowed
- No performance-hogging attacks

When you gain access, do not hinder other teams' efforts:

- Do not delete flags, data, or items
- Do not add false flags

Only the web apps on target IP range are in scope:

- Do not attack other students!!!
- XSS attacks may be placed on target web apps IF they ONLY perform XSRF or cookie theft attacks on in-scope websites

You cannot do a few things:

- **No denial-of-service attacks:** We want everyone to reach the systems.
- **No "dangerous" attacks:** We don't want to delete files and data. We also want to recognize that this is a production system, so resource-hogging attacks should not be run.

Do NOT attack other testers!

ADDITIONAL RULES OF ENGAGEMENT

You are allowed to create new accounts:
- Do not change other users' passwords

You are allowed to write to files and install software:
- Do not uninstall software or harden the applications

Remember that this is both a production system and others are testing it

When in doubt, ask

You are allowed to create accounts, but do not change other users' passwords. This may prevent another student from getting through the game.

Installing applications and writing to files is allowed, as long as the applications and files do not cause issues for the production applications. You may want to configure your injected files to answer only to your team.

Keep in mind that this is a production system and that others are also testing the applications.

CAPTURE THE FLAG GOAL

Gather all 42 flags hidden in the environment:

- Flags are a combination of their name and a hash
- Name: key99; Hash: 3228635b89112e2c641f5e5cc44e19fe

Flags can be found if you follow the methodology:

- Hidden in places you should see during mapping
- Hidden in places where you look for vulns in discovery
- Hidden behind vulnerabilities you must exploit
- Hidden deeper in the servers you must map after exploitation

You have a couple goals here. First, find as many vulnerabilities as you can. Keep in mind that not all vulnerabilities can help you retrieve the data, but they are important to your target. Evaluate the risk and explain how you can exploit any that you find.

Gather all the flags. These flags have two pieces of information. The first is a name and the second is a hash.

For example:
Name: key99
Hash: 3228635b89112e2c641f5e5cc44e19fe

This data is scattered throughout the applications and it's your job to find both.

SCORING SERVER

This CTF has a scoring server to track your progress:

- http://score.sec642.org
- Choose one person to register for a team
- Only one person can be logged in at a time
- All other members can view scores
- Coordinate keeping track of the flags

As you find flags, enter them here:

- Name
- Hash

During this CTF, there is a scoring server that can keep track of your team's score. As you find flags (the name and hash) you enter them here. You actually need to enter the two fields, and the scoreboard will validate the name and the hash.

ANY QUESTIONS?

If you have any questions, now is the time to ask!

- Ask any question you would like
- But the instructor may not answer because the purpose of the test is for you to answer some of your questions

The instructor will be available throughout the test:

- We will answer questions regarding which tool will perform which technique
- We will not tell you where the flags are
- Any hints or answers to questions will be broadcast for all to hear
- Also, the final referee and judge will declare the winners

Although any questions you have are welcome throughout the day, if you have any, ask them now. If you are wondering something, it is guaranteed that someone else also is.

The instructor will accept all questions but may not answer them because it may reveal too much information. They will be available throughout the day.

THE MANTRA

During any penetration test or CTF, always keep these things in mind:

- Where are you in the methodology
- What do you know
- What is the objective
- Which technique will achieve the goals
- Which tool performs that technique in this application

We have seen too many pen testers and teams miss things, try random tools, or overthink

Some things to think about as you go through the CTF, and later when you are performing penetration testing.

YOU NOW HAVE PERMISSION TO BEGIN

You now have permission to begin the attack against the target applications:

- 10.42.6.2-253

Follow the Rules of Engagement

If and when you win, notify the instructor:

- Don't forget to watch the scoring server

Have fun!

You now have permission to begin the attack against the target applications on 10.42.6.2-253

Follow the Rules of Engagement.

If and when you win, notify the instructor.

Have fun!

COURSE RESOURCES AND CONTACT INFORMATION

AUTHOR CONTACT
Justin Searle
justin@meeas.com
@meeas
Adrien de Beaupré
adriendb@gmail.com
@adriendb

SANS INSTITUTE
11200 Rockville Pike, Suite 200
North Bethesda, MD 20852
301.654.SANS(7267)

PEN TESTING RESOURCES
pen-testing.sans.org
Twitter: @SANSPenTest

SANS EMAIL
GENERAL INQUIRIES: info@sans.org
REGISTRATION: registration@sans.org
TUITION: tuition@sans.org
PRESS/PR: press@sans.org

Please use our hashtag #SEC642 and follow us on Twitter!

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

P

Q

R

S

T

U

V

W

X

Y

Z