SANS

www.sans.org

SECURITY 642

ADVANCED WEB APP PENETRATION TESTING AND ETHICAL HACKING

642.6

Capture the Flag

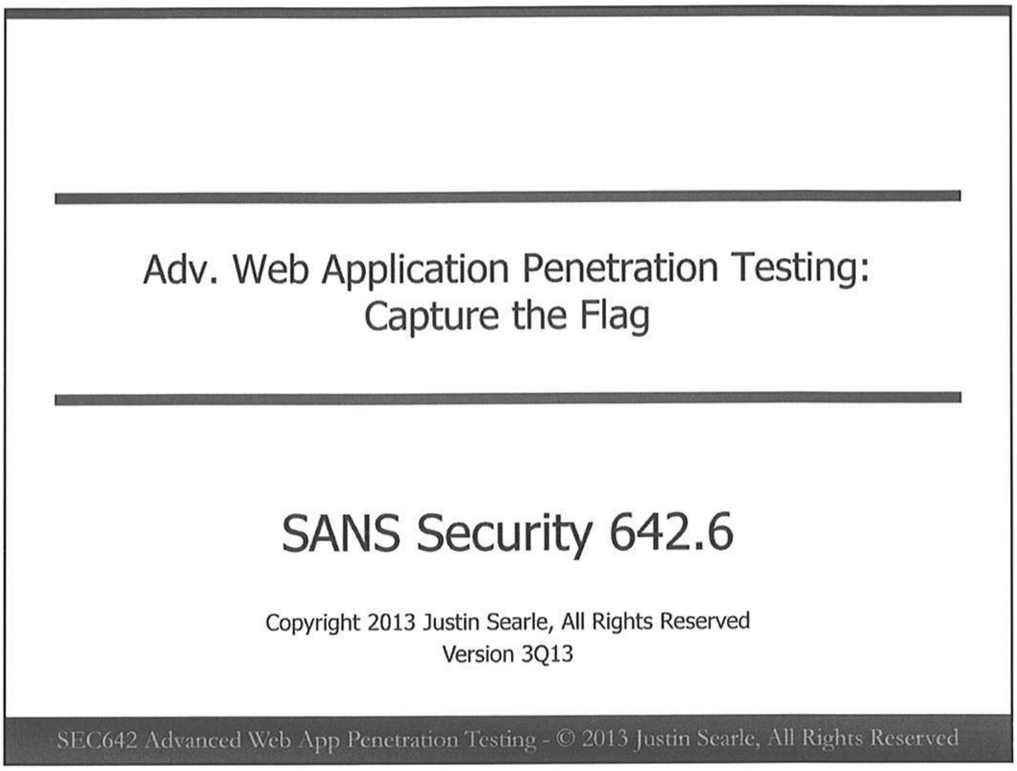
The right security training for your staff, at the right time, in the right location.

IMPORTANT-READ CAREFULLY:

This Courseware License Agreement ("CLA") is a legal agreement between you (either an individual or a single entity; henceforth User) and the SANS Institute for the personal, non-transferable use of this courseware. User agrees that the CLA is the complete and exclusive statement of agreement between The SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA. If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this courseware. BY ACCEPTING THIS COURSEWARE YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. IF YOU DO NOT AGREE YOU MAY RETURN IT TO THE SANS INSTITUTE FOR A FULL REFUND, IF APPLICABLE. The SANS Institute hereby grants User a non-exclusive license to use the material contained in this courseware subject to the terms of this agreement. User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of this publication in any medium whether printed, electronic or otherwise, for any purpose without the express written consent of the SANS Institute. Additionally, user may not sell, rent, lease, trade, or otherwise transfer the courseware in any way, shape, or form without the express written consent of the SANS Institute.

The SANS Institute reserves the right to terminate the above lease at any time. Upon termination of the lease, user is obligated to return all materials covered by the lease within a reasonable amount of time.

V2013_0902

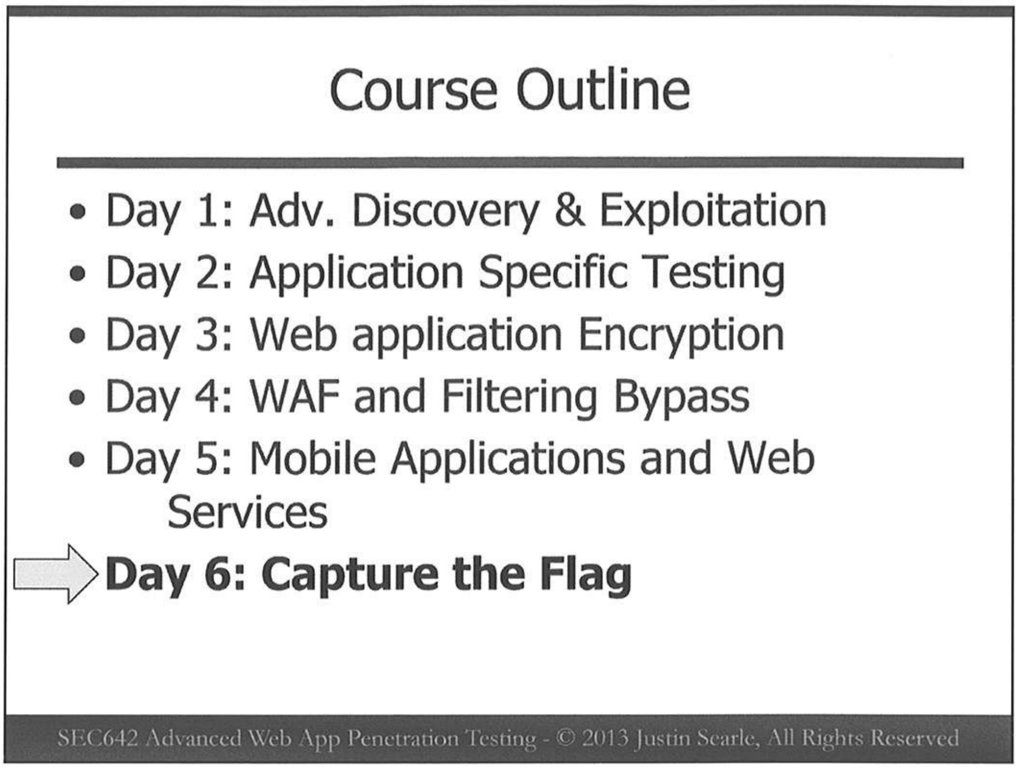


Adv. Web Application Penetration Testing: Capture the Flag

SANS Security 642.6

Version 3Q13

This page intentionally left blank.

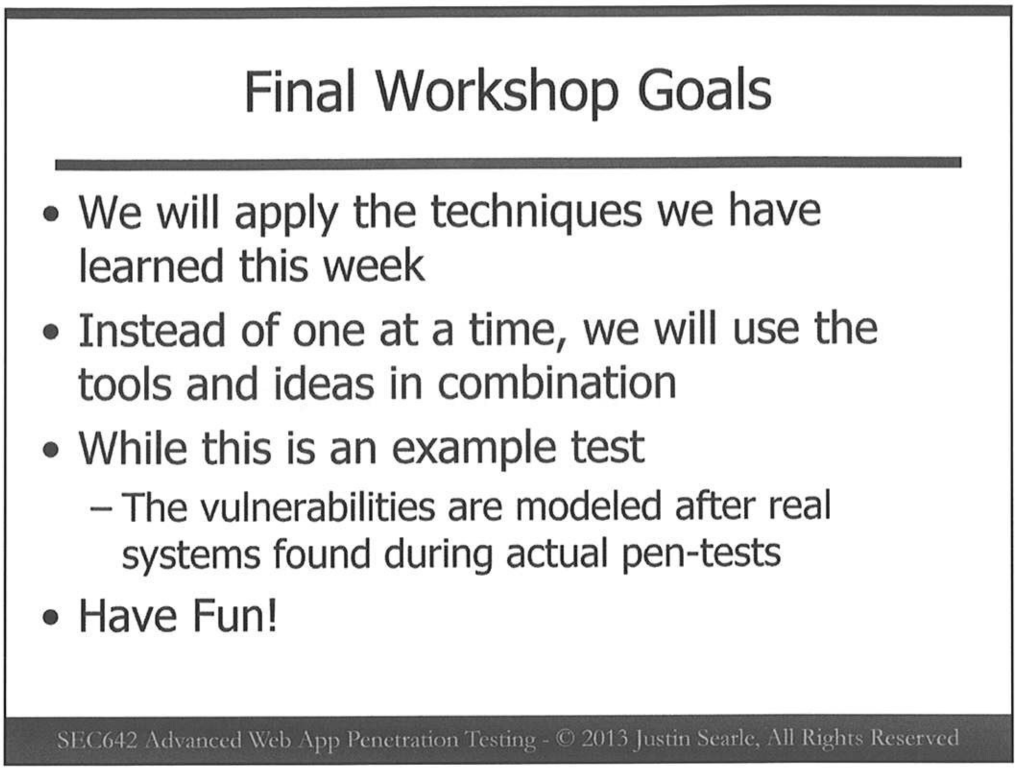


Course Outline

- Day 1: Adv. Discovery & Exploitation
- Day 2: Application Specific Testing
- Day 3: Web application Encryption
- Day 4: WAF and Filtering Bypass
- Day 5: Mobile Applications and Web Services

⇨ **Day 6: Capture the Flag**

This page intentionally left blank.



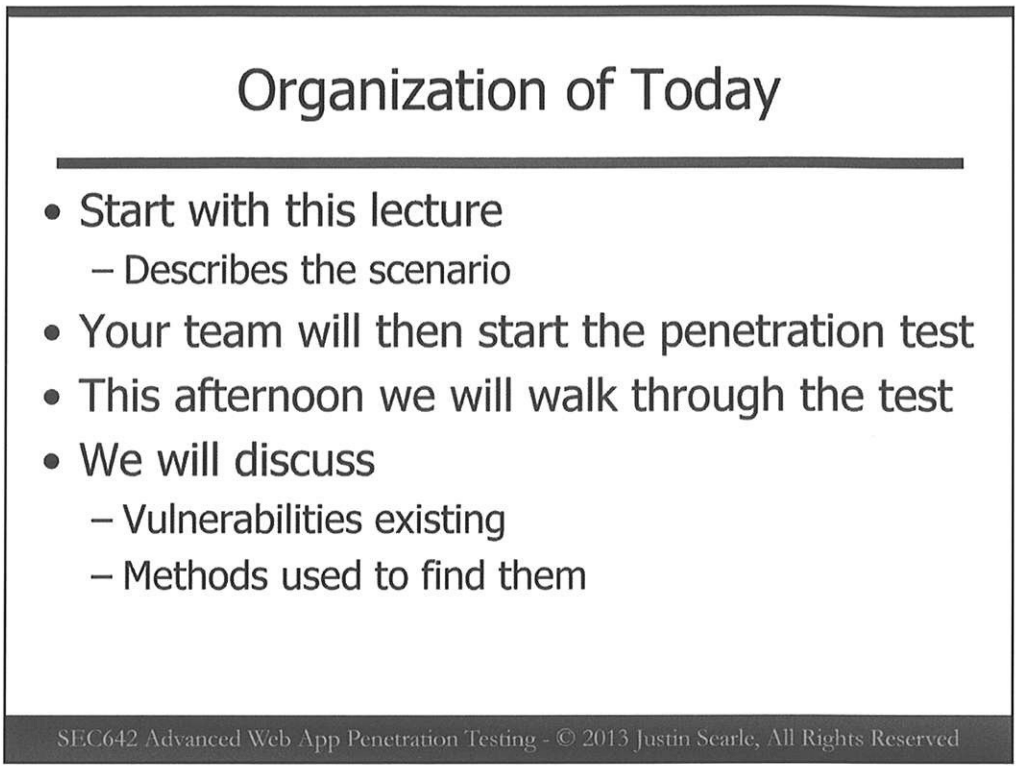
Final Workshop Goals

- We will apply the techniques we have learned this week
- Instead of one at a time, we will use the tools and ideas in combination
- While this is an example test
  - The vulnerabilities are modeled after real systems found during actual pen-tests
- Have Fun!

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

While the test we are doing is an example, it is based on real vulnerabilities and applications we have found 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.

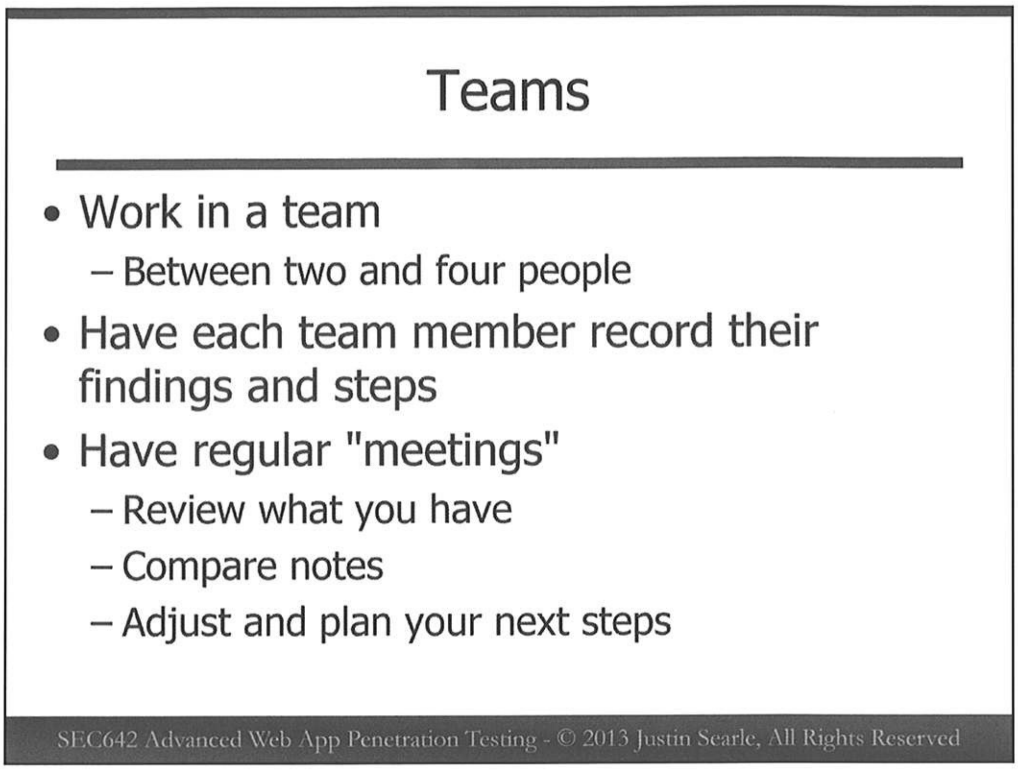
Most importantly, please have fun!



Organization of Today

- Start with this lecture
  - Describes the scenario
- Your team will then start the penetration test
- This afternoon we will walk through the test
- We will discuss
  - Vulnerabilities existing
  - Methods used to find them

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



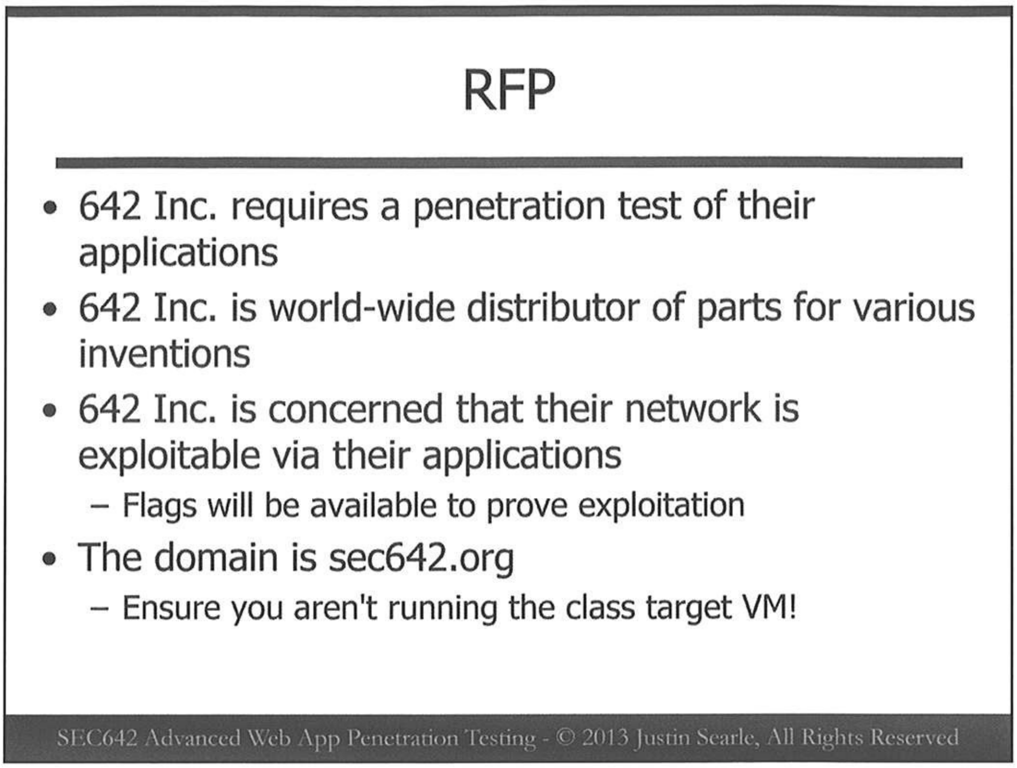
Teams

- Work in a team
  - Between two and four people
- Have each team member record their findings and steps
- Have regular "meetings"
  - Review what you have
  - Compare notes
  - Adjust and plan your next steps

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

Have each person record their findings and steps. After class, these notes would be useful for review.

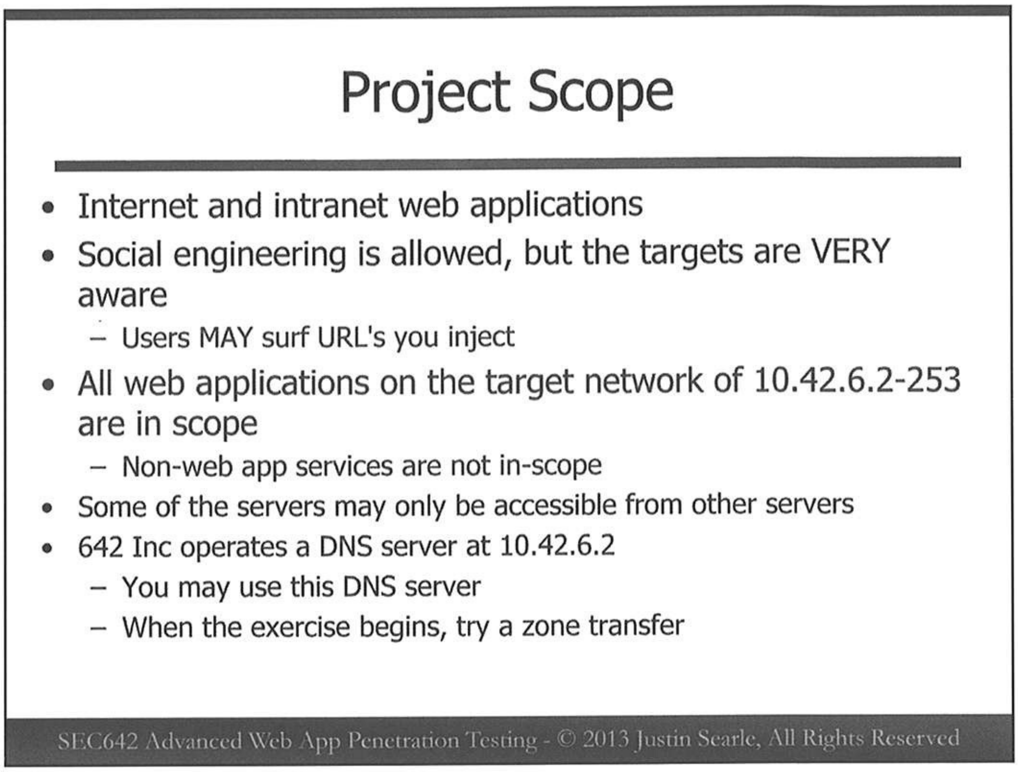
But make sure that you have regular meetings to compare notes and make sure that you are working together. This is VERY important, we see too often where people on a team will have pieces of what is needed, but they don't talk to each other.



RFP

- 642 Inc. requires a penetration test of their applications
- 642 Inc. is world-wide distributor of parts for various inventions
- 642 Inc. is concerned that their network is exploitable via their applications
  - Flags will be available to prove exploitation
- The domain is sec642.org
  - Ensure you aren't running the class target VM!

642 Inc. has put out an RFP for a web application penetration test. They are concerned that their network can be compromised via their applications. Our job is to test and find these flaws. We will be targeting the entire sec642.org domain and will be looking for various flags to prove our exploits.

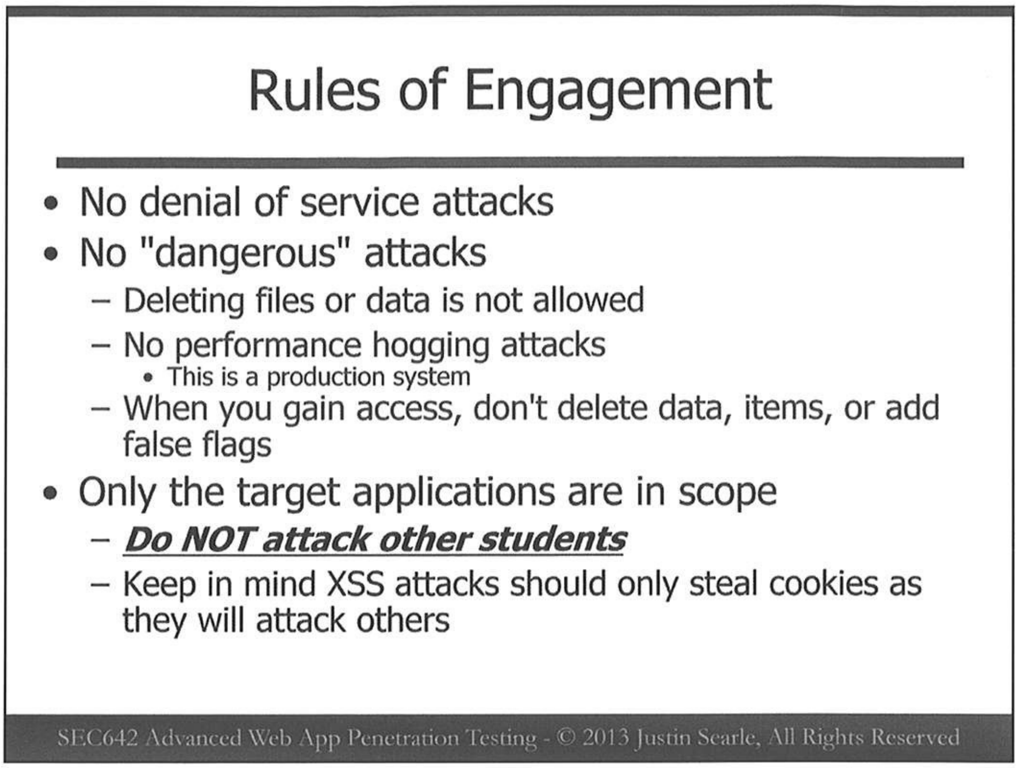


Project Scope

- Internet and intranet web applications
- Social engineering is allowed, but the targets are VERY aware
  - Users MAY surf URL's you inject
- All web applications on the target network of 10.42.6.2-253 are in scope
  - Non-web app services are not in-scope
- Some of the servers may only be accessible from other servers
- 642 Inc operates a DNS server at 10.42.6.2
  - You may use this DNS server
  - When the exercise begins, try a zone transfer

To determine the risk level of having this information disclosed, they have requested a test of all of their web applications. This included Internet and intranet facing applications. Social engineering is allowed but keep in mind that the target is very security conscious and aware of the ongoing test. But 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 that you should use for the test.



Rules of Engagement

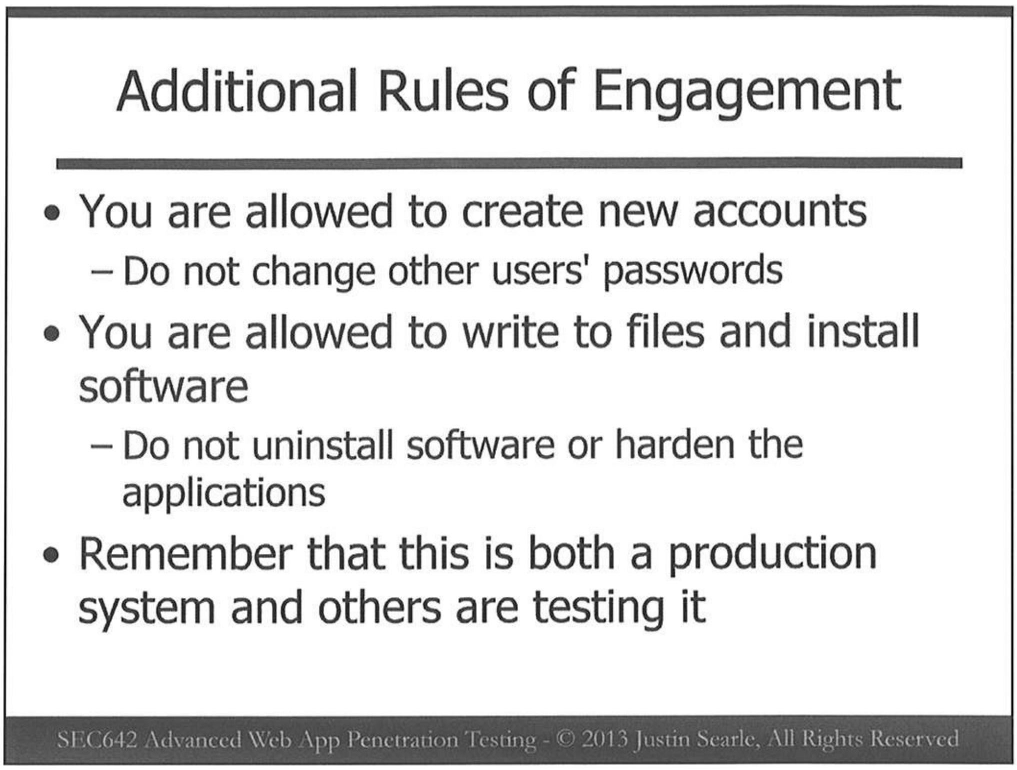
- No denial of service attacks
- No "dangerous" attacks
  - Deleting files or data is not allowed
  - No performance hogging attacks
    - This is a production system
  - When you gain access, don't delete data, items, or add false flags
- Only the target applications are in scope
  - ***Do NOT attack other students***
  - Keep in mind XSS attacks should only steal cookies as they will attack others

There are a few things you cannot do.

No denial of service attacks. We want everyone to be able to reach the systems.

No "dangerous" attacks. We don't want to delete files and/or 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!



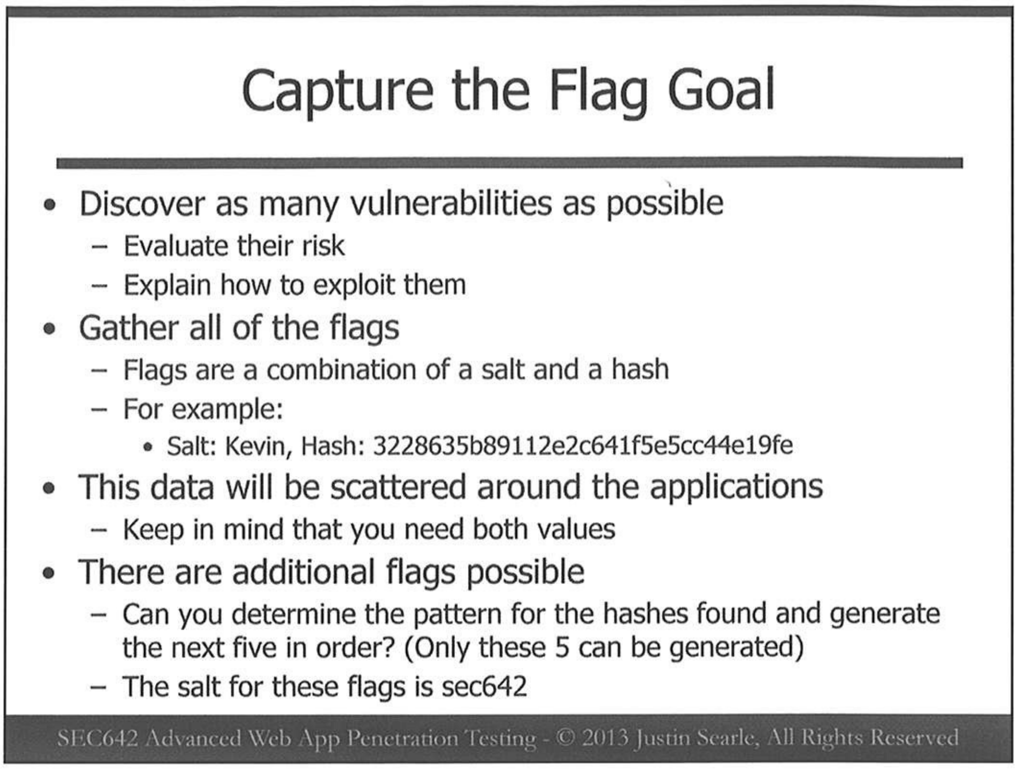
Additional Rules of Engagement

- 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

You are allowed to create accounts, but please 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 only answer to your team. ☺

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



Capture the Flag Goal

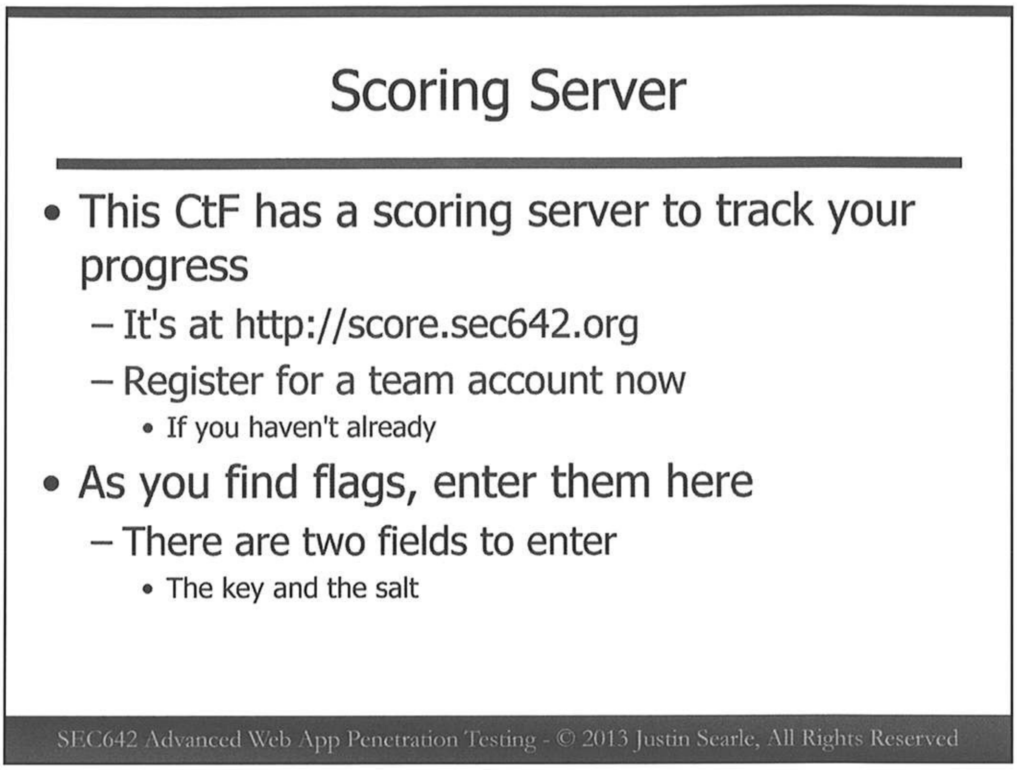
- Discover as many vulnerabilities as possible
  - Evaluate their risk
  - Explain how to exploit them
- Gather all of the flags
  - Flags are a combination of a salt and a hash
  - For example:
    - Salt: Kevin, Hash: 3228635b89112e2c641f5e5cc44e19fe
- This data will be scattered around the applications
  - Keep in mind that you need both values
- There are additional flags possible
  - Can you determine the pattern for the hashes found and generate the next five in order? (Only these 5 can be generated)
  - The salt for these flags is sec642

You have a couple goals here. First, find as many vulnerabilities as you can. Please keep in mind that not all vulnerabilities will 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 of the flags. These flags have two pieces of information. The first is a salt and the second is a hash. For example: Salt: Kevin, Hash: 3228635b89112e2c641f5e5cc44e19fe .

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

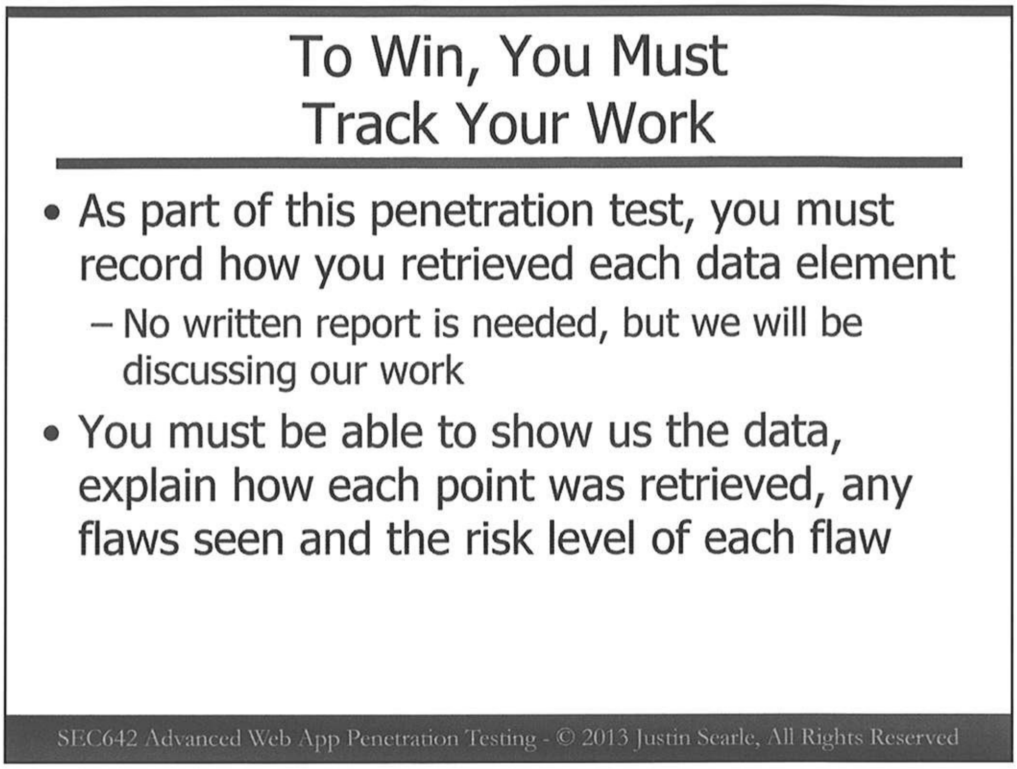
There are additional flags for extra points. These flags are based on the fact that the rest of the hashes are based on a pattern. If you can determine what this is, enter it into the scoring server. The salt to use is sec642 .



Scoring Server

- This CtF has a scoring server to track your progress
  - It's at http://score.sec642.org
  - Register for a team account now
    - If you haven't already
- As you find flags, enter them here
  - There are two fields to enter
    - The key and the salt

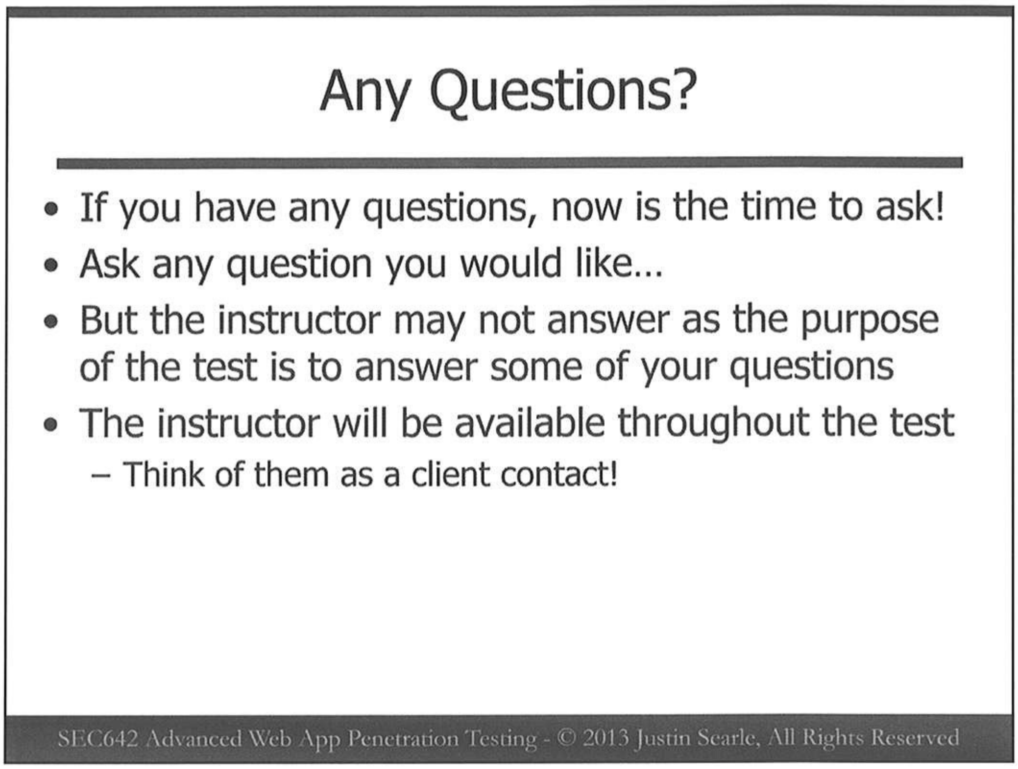
During this CtF, there is a scoring server which is used to keep track of your team's score. As you find flags, the salt and hash, you will enter them here. Keep in mind that you will actually be entering the two fields and the scoreboard will generate a hash that is generated from the salt and the hash.



To Win, You Must Track Your Work

- As part of this penetration test, you must record how you retrieved each data element
  - No written report is needed, but we will be discussing our work
- You must be able to show us the data, explain how each point was retrieved, any flaws seen and the risk level of each flaw

You must also track your work! Keep records as to how you retrieved each data element and all of the vulnerabilities you find. While you are not required to present a written report, the instructor will quiz you to ensure that you could explain what you found, did and the risks seen.

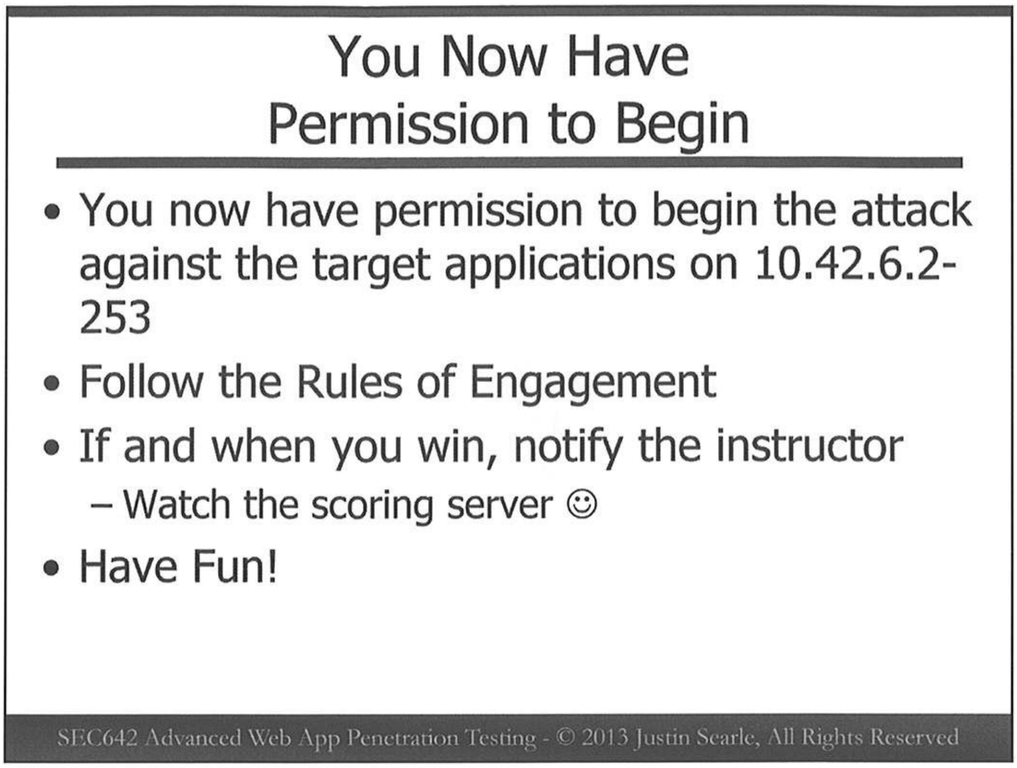


Any Questions?

- If you have any questions, now is the time to ask!
- Ask any question you would like…
- But the instructor may not answer as the purpose of the test is to answer some of your questions
- The instructor will be available throughout the test
  - Think of them as a client contact!

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

The instructor will accept any question, but they may not be able to answer them as it may reveal too much information. Treat them as you would your customer contact. They will be available throughout the day.



You Now Have Permission to Begin

- 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
  - 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!