© SANS Institute 2019

SEC575 | MOBILE DEVICE SECURITY AND ETHICAL HACKING

575.6

Capture the Flag

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

© SANS Institute 2019

Copyright © 2019 Joshua Wright and NVISO. All rights reserved to Joshua Wright, NVISO, and/or SANS Institute.

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE “USER”) AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between 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.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of 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 SANS Institute.

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.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There’s an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

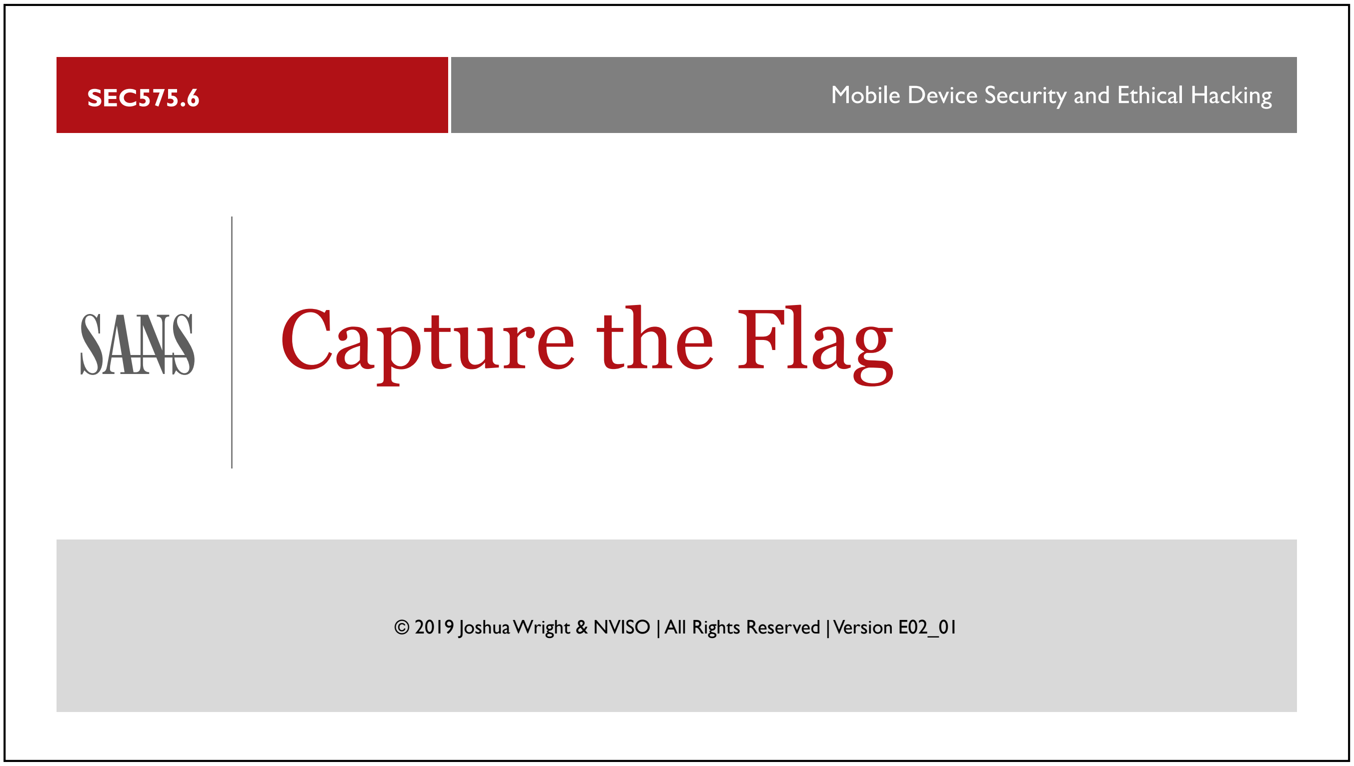
PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

© SANS Institute 2019



SEC575.6

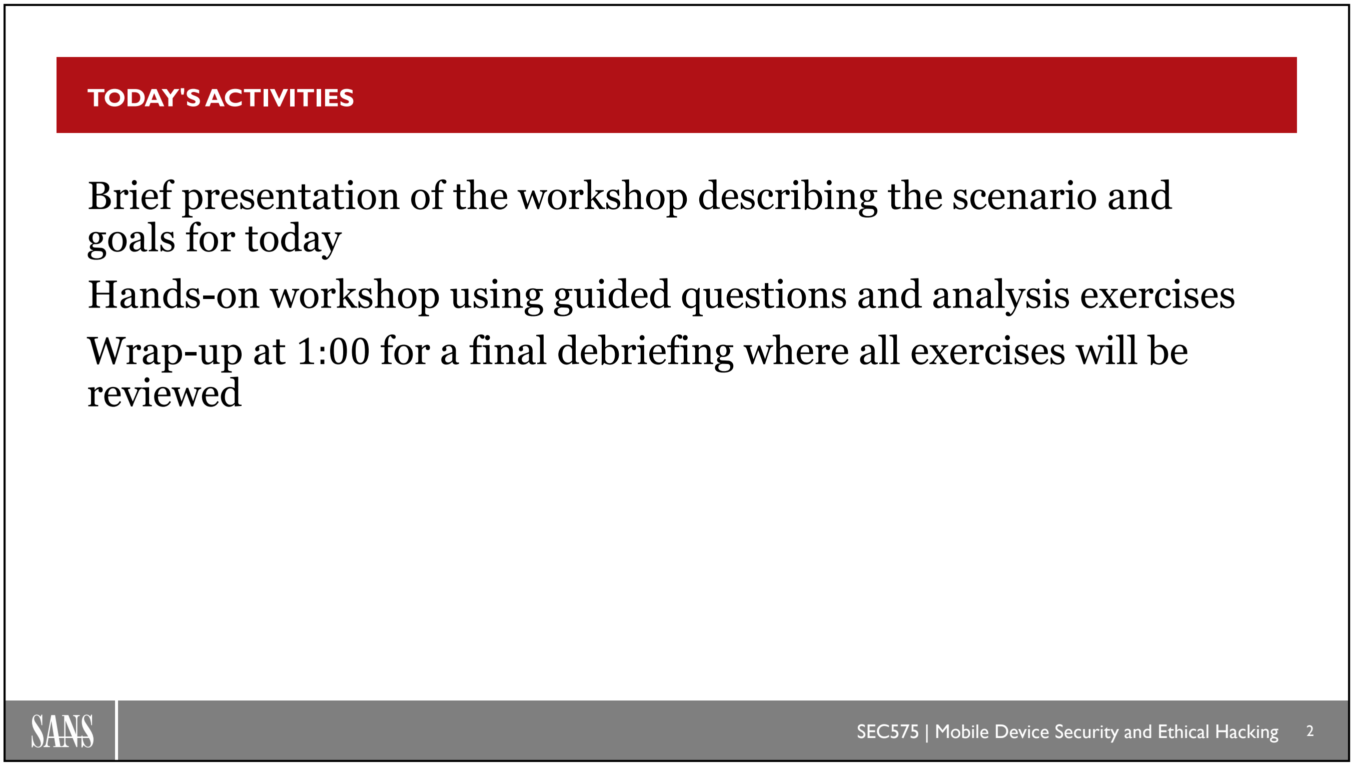
Mobile Device Security and Ethical Hacking

Capture the Flag

© 2019 Joshua Wright & NVISO | All Rights Reserved | Version E02_01

Welcome to SANS Security 575.6. Today you will work individually or as part of a team to complete a series of challenges that closely resemble the responsibilities of a lead mobile device security analyst. This final book in the 575 series describes the challenge you will be facing, provides the Rules of Engagement, and provides a description of how to conduct the exercise. This session will center on the hands-on application of tools and techniques we've discussed throughout the class.

© SANS Institute 2019



TODAY'S ACTIVITIES

Brief presentation of the workshop describing the scenario and goals for today

Hands-on workshop using guided questions and analysis exercises

Wrap-up at 1:00 for a final debriefing where all exercises will be reviewed

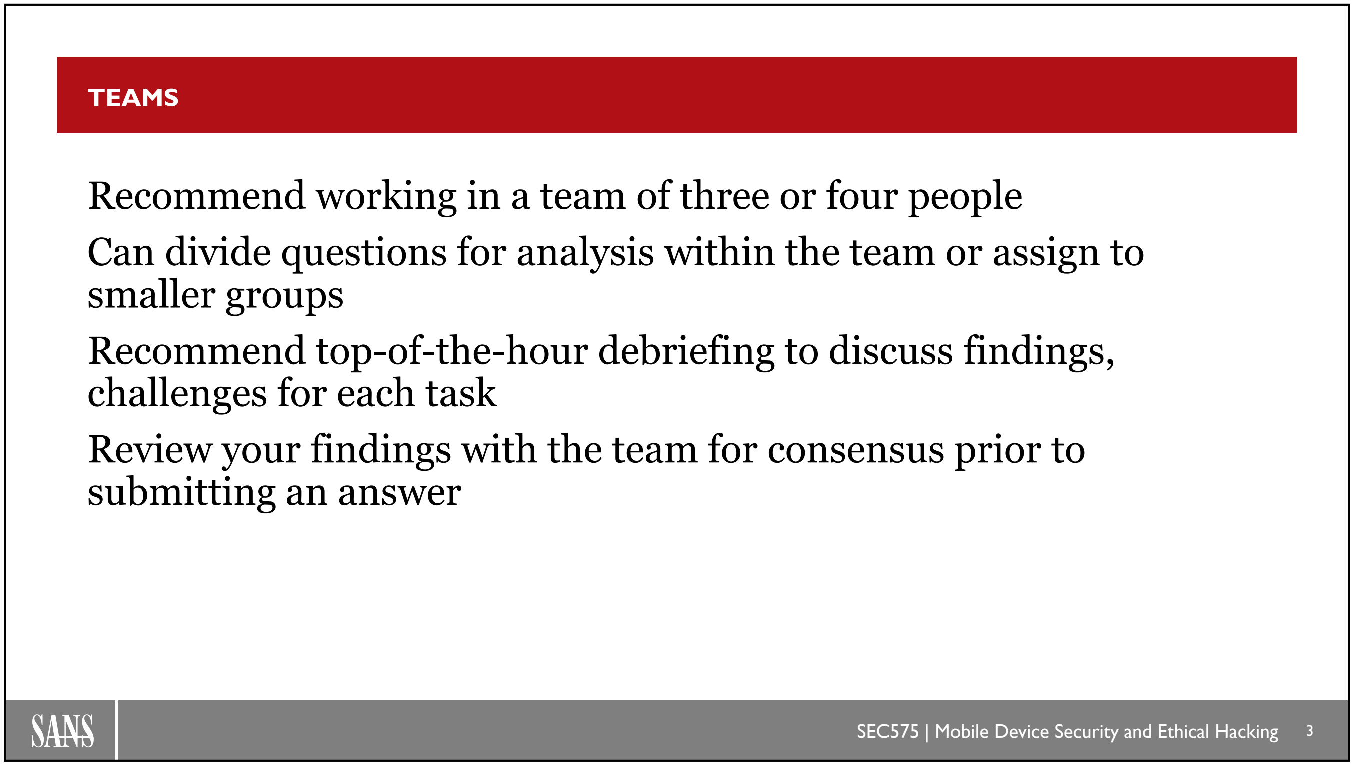
Today's Activities

Today we'll be participating in the hands-on final workshop event. First, we'll start with a brief presentation of the workshop describing the scenario we've outlined and the goals for today. This presentation will take approximately 30 minutes.

Once the presentation is complete, you will start the hands-on workshop using guided questions and analysis exercises. This will take the majority of the time today, stopping at 1:00 p.m. for a final debriefing. During this debriefing, all the exercises will be reviewed and questions will be answered.

© 2019 Joshua Wright & NVISO

© SANS Institute 2019



TEAMS

- Recommend working in a team of three or four people
- Can divide questions for analysis within the team or assign to smaller groups
- Recommend top-of-the-hour debriefing to discuss findings, challenges for each task
- Review your findings with the team for consensus prior to submitting an answer

SANS SEC575 | Mobile Device Security and Ethical Hacking 3

Teams

For the best workshop experience, we recommend that everyone work in teams of three to four people. Within the team, you can work together with other analysts to answer questions and complete analysis tasks as a single team (each person working on the same question) or divide up the responsibilities of the team with smaller groups to assess some of the more complex analysis tasks in parallel.

We also recommend that each team take a 5–10-minute break at the top of every hour to discuss findings, challenges, and problem areas for each task. Talking a problem out with other people on the team can be a tremendously useful exercise, allowing you to take a step back from the problem while seeking the advice of other analysts.

Prior to submitting the answer to a question or analysis task, we recommend that the team review the answer as a whole and approve the response. This will help avoid the loss of points from the submission of incorrect answers.

© SANS Institute 2019

YOUR POSITION

You are the chief mobile device security analyst for Gamera Aeronautic Systems Corporation (GAS)

You and your team are responsible for multiple facets of a mobile device deployment

The GAS CSO, Mike Hottaire, has assigned your team several tasks to complete

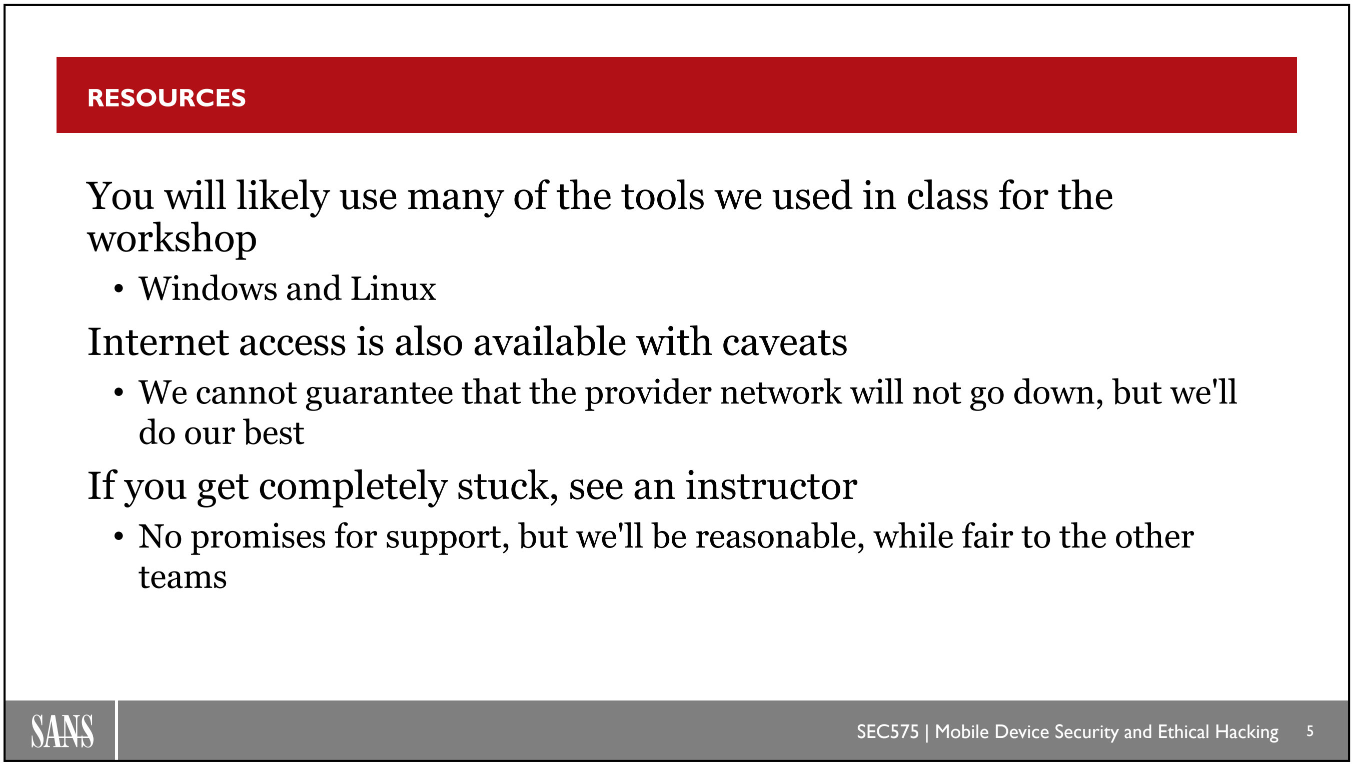
- Including analysis and penetration testing tasks

Your Position

In this workshop, you are the chief mobile device security analyst for Gamera Aeronautic Systems Corporation (GAS). You and your team are responsible for multiple facets of a mobile device deployment, reporting to the GAS CSO, Mike Hottaire. Mike has assigned your team several tasks to complete, ranging from simple question-and-answer tasks to more complex analysis and penetration tasks.

© 2019 Joshua Wright & NVISO

© SANS Institute 2019



RESOURCES

You will likely use many of the tools we used in class for the workshop

- Windows and Linux

Internet access is also available with caveats

- We cannot guarantee that the provider network will not go down, but we'll do our best

If you get completely stuck, see an instructor

- No promises for support, but we'll be reasonable, while fair to the other teams

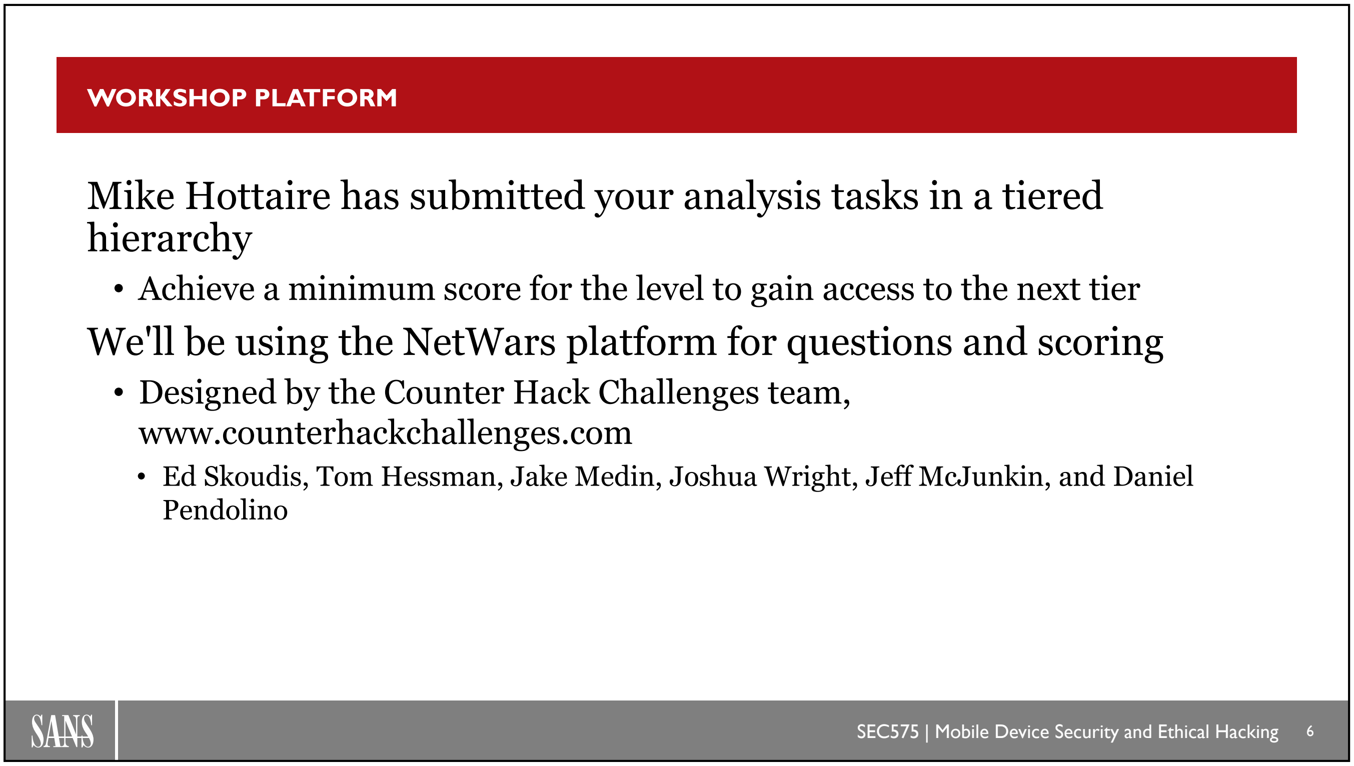
Resources

To complete the analysis tasks Mike has assigned to you, you will use many of the tools we used in the course. You will likely use both Windows and Linux for the analysis tasks.

Throughout the workshop, you will also have access to the internet, with caveats. Notably, we cannot guarantee that the provider network will not go down during the workshop, but we will do our best to ensure you have access to internet search engines and other online resources.

If you and your team get completely stuck on an analysis exercise, please see an instructor for assistance. We are not promising to give you hints or answers, but we'll be reasonable in providing guidance while being fair to the other teams.

© SANS Institute 2019



WORKSHOP PLATFORM

Mike Hottaire has submitted your analysis tasks in a tiered hierarchy

- Achieve a minimum score for the level to gain access to the next tier

We'll be using the NetWars platform for questions and scoring

- Designed by the Counter Hack Challenges team, www.counterhackchallenges.com
  - Ed Skoudis, Tom Hessman, Jake Medin, Joshua Wright, Jeff McJunkin, and Daniel Pendolino

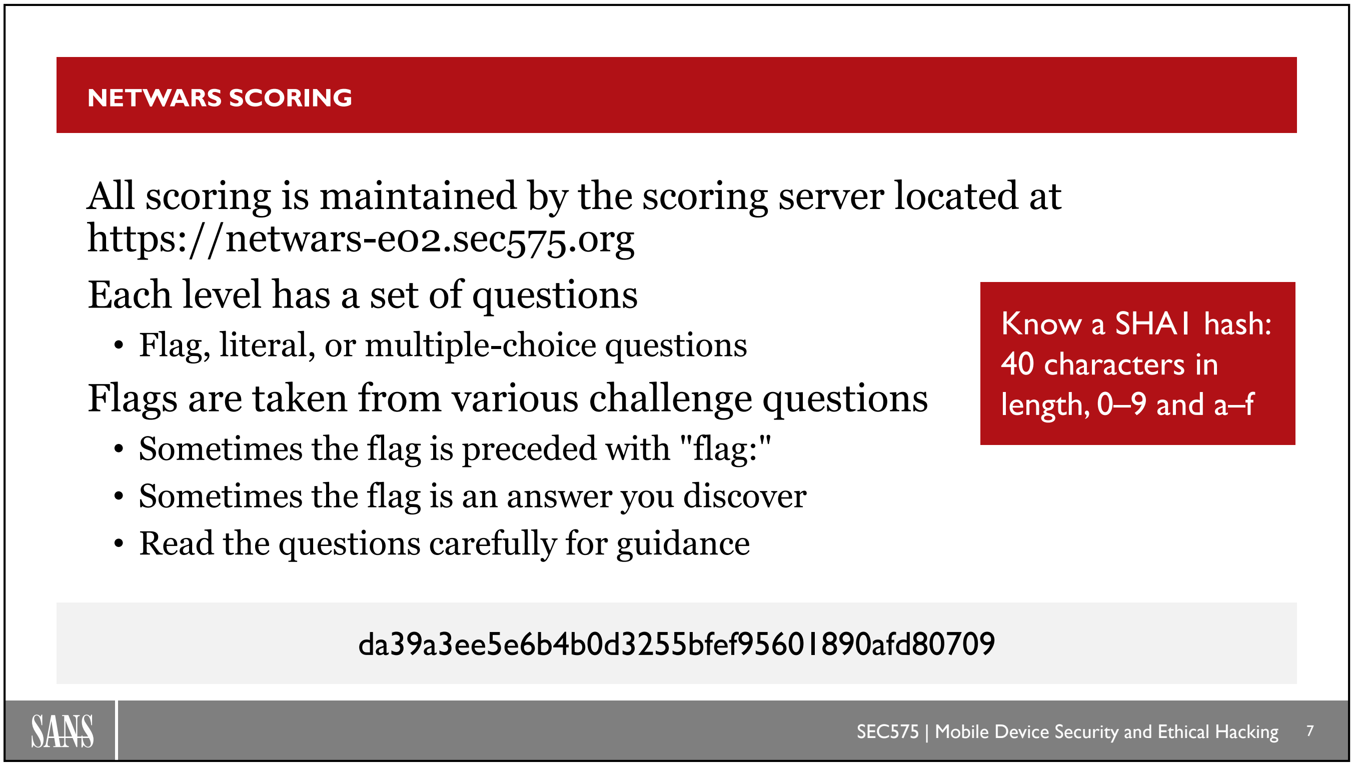
Workshop Platform

GAS CSO Mike Hottaire has submitted the analysis tasks you need to complete in a tiered hierarchy. You'll start with Level 1 questions, moving up to the next level after achieving a minimum score defined for each level.

Throughout the workshop, we'll use the NetWars platform for the delivery of questions and validation of responses, as well for scoring each team. The NetWars platform was designed by the Counter Hack Challenges team (www.counterhackchallenges.com) consisting of Ed Skoudis, Tom Hessman, Jake (Tim) Medin, Joshua Wright, Jeff McJunkin, and Daniel Pendolino.

© 2019 Joshua Wright & NVISO

© SANS Institute 2019



NETWARS SCORING

All scoring is maintained by the scoring server located at https://netwars-e02.sec575.org

Each level has a set of questions

- Flag, literal, or multiple-choice questions

Flags are taken from various challenge questions

- Sometimes the flag is preceded with "flag:"
- Sometimes the flag is an answer you discover
- Read the questions carefully for guidance

Know a SHA1 hash: 40 characters in length, 0–9 and a–f

da39a3ee5e6b4b0d3255bfef95601890afd80709

NetWars Scoring

All scoring in the workshop is maintained by the scoring server at https://netwars-e02.sec575.org. After logging into the scoring server, you will see the questions for your level achievement and be able to submit your responses. Your answers to the questions will gain or cost you points. You can also monitor the score of other teams from the scoring server as well.

Each level in the workshop has a set of questions you will answer. Some questions will be multiple choice, but many will require an answer that represents a literal value (such as a word or a group of words) or a flag. Flags are taken from the various challenge questions, sometimes preceded with the string "flag:". Sometimes a flag is a string or other answer you discover by completing the analysis task. Read each question carefully for guidance on what should be submitted for the answer.

Some exercises will require you to find a flag value in a file, program, or other network resource. Flags are in SHA1 hash format, as shown on this page. The SHA1 flags are 40 characters in length, consisting of hexadecimal characters (0–9 and a–f).

© SANS Institute 2019

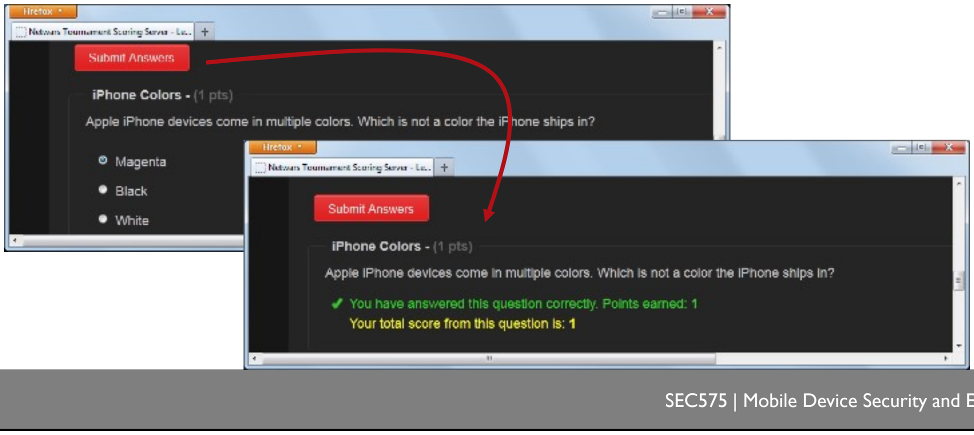
SAMPLE QUESTION (1)

Multiple questions are listed per level

Answer any question and click Submit

- Unanswered questions are ignored

Order of answers changes for multiple-choice questions!


Firefox
Netwars Tournament Scoring Server - Lo...
Submit Answers

iPhone Colors - (1 pts)

Apple iPhone devices come in multiple colors. Which is not a color the iPhone ships in?

○ Magenta
● Black
● White

Firefox
Netwars Tournament Scoring Server - Lo...
Submit Answers

iPhone Colors - (1 pts)

Apple iPhone devices come in multiple colors. Which is not a color the iPhone ships in?

✓ You have answered this question correctly. Points earned: 1

Your total score from this question is: 1

Sample Question (1)

This page has an example question from the NetWars scoring engine. The participant reviews the question and selects the answer he or she thinks is correct. At any time, there will be multiple questions that are accessible; answer the question and submit your answer by clicking the "Submit Answers" button. You can answer one or more questions each time you click submit; questions that have not been answered are ignored by the scoring engine, allowing you to answer them at a later time.

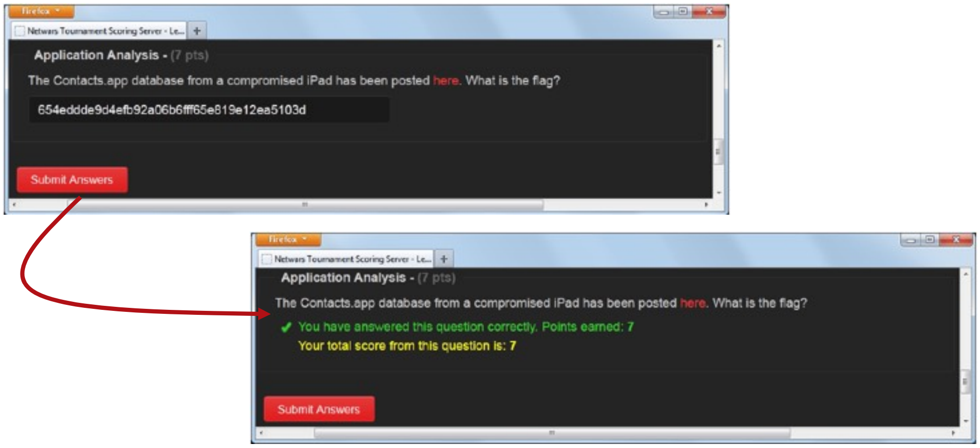
Note that for multiple-choice questions, the order of answers will change each time the page is retrieved (and for different people on the same team).

© 2019 Joshua Wright & NVISO

© SANS Institute 2019

SAMPLE QUESTION (2)

Some questions will ask for a flag (40 characters) or a literal value



Application Analysis - (7 pts)

The Contacts.app database from a compromised iPad has been posted here. What is the flag?

654eddde9d4efb92a06b6fff65e819e12ea5103d

Application Analysis - (7 pts)

The Contacts.app database from a compromised iPad has been posted here. What is the flag?

✓ You have answered this question correctly. Points earned: 7

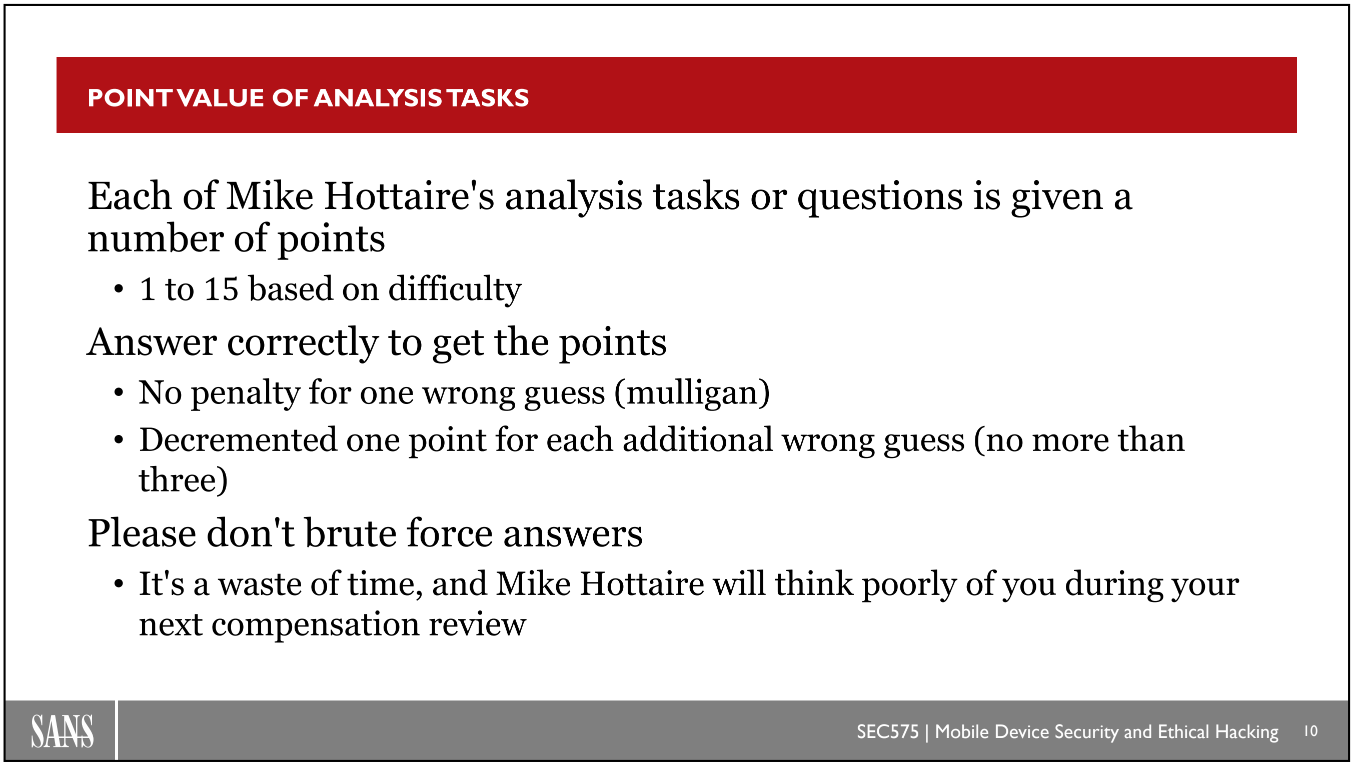
Your total score from this question is: 7

Sample Question (2)

The sample question on this page is a flag question where the participant is challenged to gather data from a linked resource and identify the flag. Remember that flag values are 40-character SHA1 hashes, as shown here.

Other questions will require a literal value, such as one or more words, an IP address, or any other string value.

© SANS Institute 2019



POINT VALUE OF ANALYSIS TASKS

Each of Mike Hottaire's analysis tasks or questions is given a number of points

- 1 to 15 based on difficulty

Answer correctly to get the points

- No penalty for one wrong guess (mulligan)
- Decremented one point for each additional wrong guess (no more than three)

Please don't brute force answers

- It's a waste of time, and Mike Hottaire will think poorly of you during your next compensation review

Point Value of Analysis Tasks

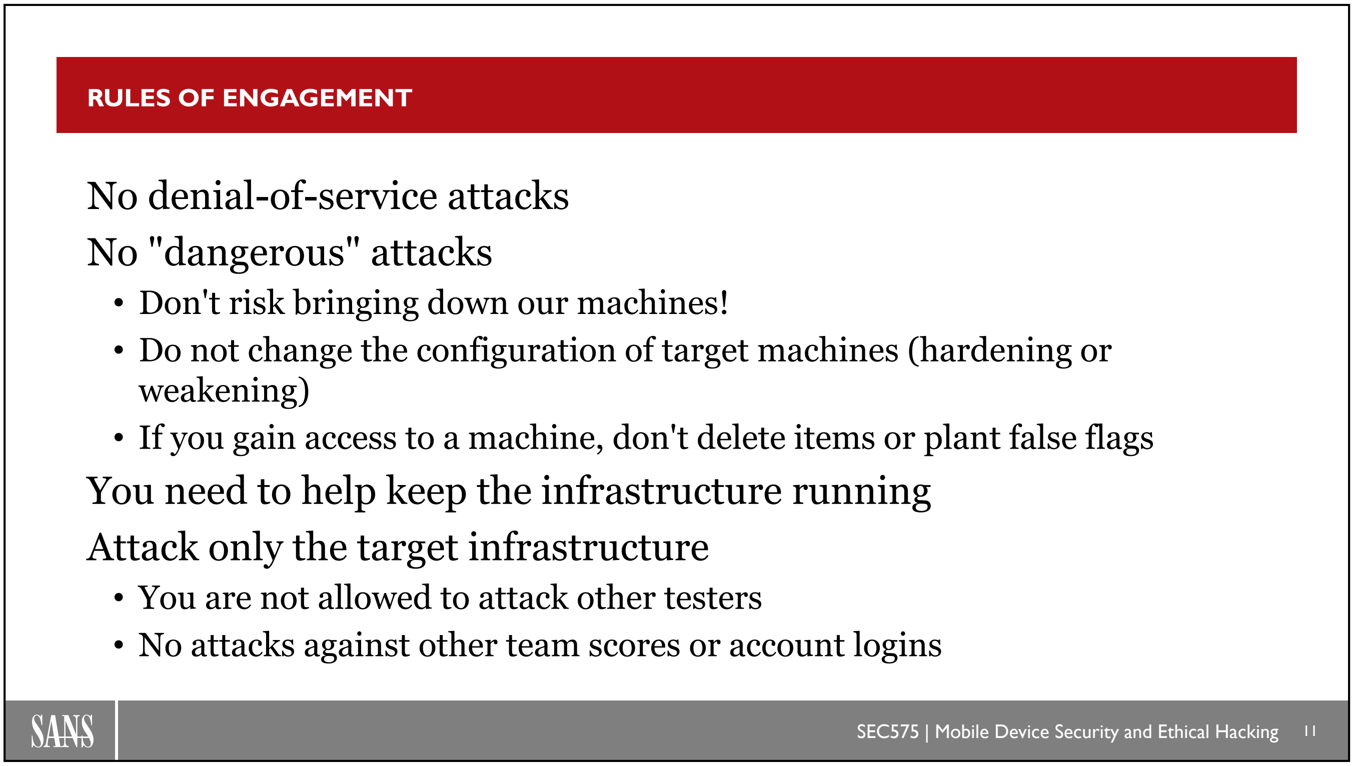
Each of Mike Hottaire's analysis tasks or questions is assigned a number of points between 1 and 15 that are rewarded for a correct answer. Answer a question correctly to gain the point value assigned to the question.

The first wrong answer for each question will not decrement points. Additional wrong answers for each question will decrement one point for each incorrect response, up to three points total.

Please don't attempt to brute force the answers. It is not permitted within the scope of this workshop and, furthermore, will make Mike Hottaire think less of you.

© 2019 Joshua Wright & NVISO

© SANS Institute 2019



RULES OF ENGAGEMENT

No denial-of-service attacks

No "dangerous" attacks

- Don't risk bringing down our machines!
- Do not change the configuration of target machines (hardening or weakening)
- If you gain access to a machine, don't delete items or plant false flags

You need to help keep the infrastructure running

Attack only the target infrastructure

- You are not allowed to attack other testers
- No attacks against other team scores or account logins

SANS

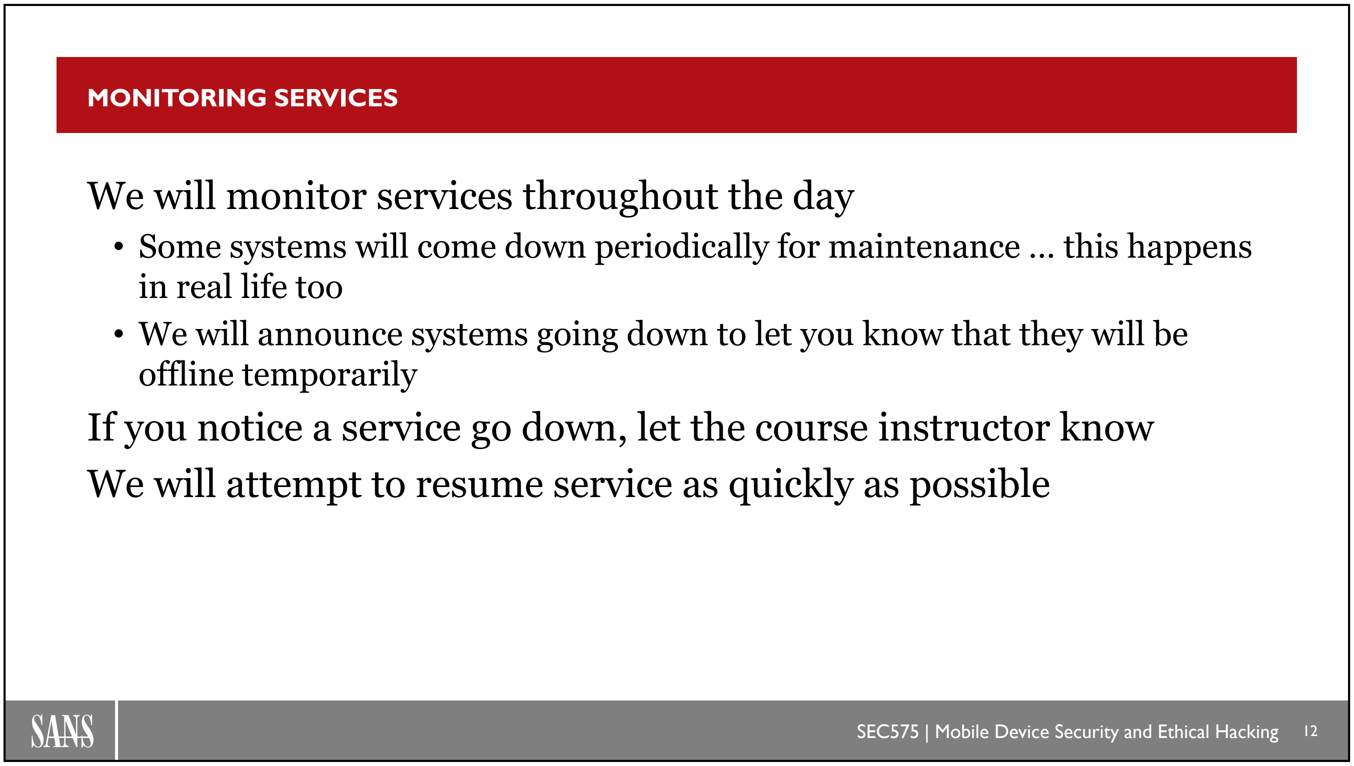
SEC575 | Mobile Device Security and Ethical Hacking 11

Rules of Engagement

During this workshop, participants are forbidden from performing denial-of-service attacks or otherwise dangerous attacks that threaten the stability of the systems supporting the assessment. Do not risk bringing down our machines and avoid excessive system use (such as excessive disk I/O or CPU-intensive activities). If you gain access to a system, don't delete items or plant false flags on the system. We need your help to keep the workshop infrastructure running!

In the workshop, you are allowed to attack only the target infrastructure identified in the question presented by the scoring server. You are not allowed to attack other testers on your team or other teams. You are not allowed to attack the scoring server, including any attempts to access other team scores or account logins.

© SANS Institute 2019



MONITORING SERVICES

We will monitor services throughout the day

- Some systems will come down periodically for maintenance … this happens in real life too
- We will announce systems going down to let you know that they will be offline temporarily

If you notice a service go down, let the course instructor know

We will attempt to resume service as quickly as possible

SEC575 | Mobile Device Security and Ethical Hacking 12

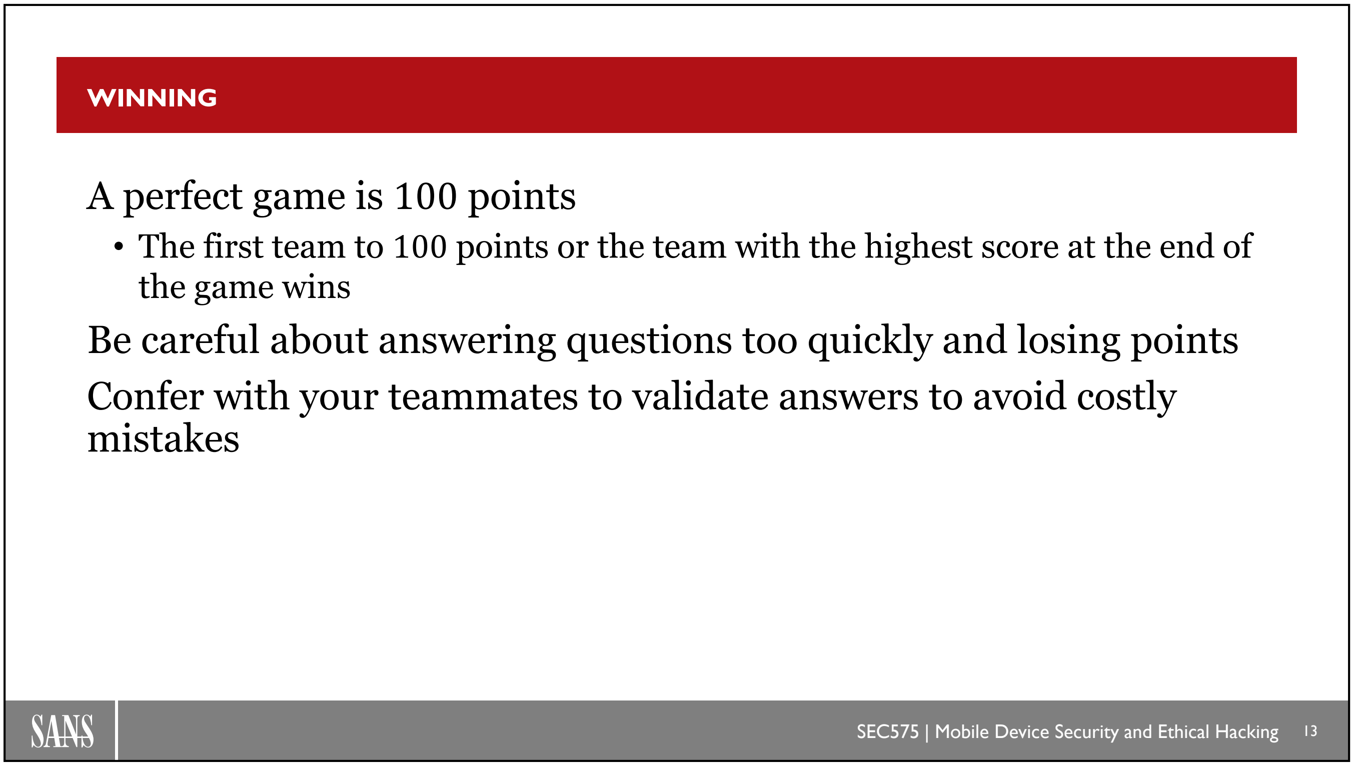
Monitoring Services

Throughout the day, we will monitor services supporting the workshop to ensure their availability. We might need to take systems temporarily offline to restore their functionality and will notify the workshop participants accordingly.

If you notice a service that goes down, let the course instructor know. We will attempt to resume service as quickly as possible.

© 2019 Joshua Wright & NVISO

© SANS Institute 2019



WINNING

A perfect game is 100 points

- The first team to 100 points or the team with the highest score at the end of the game wins

Be careful about answering questions too quickly and losing points

Confer with your teammates to validate answers to avoid costly mistakes

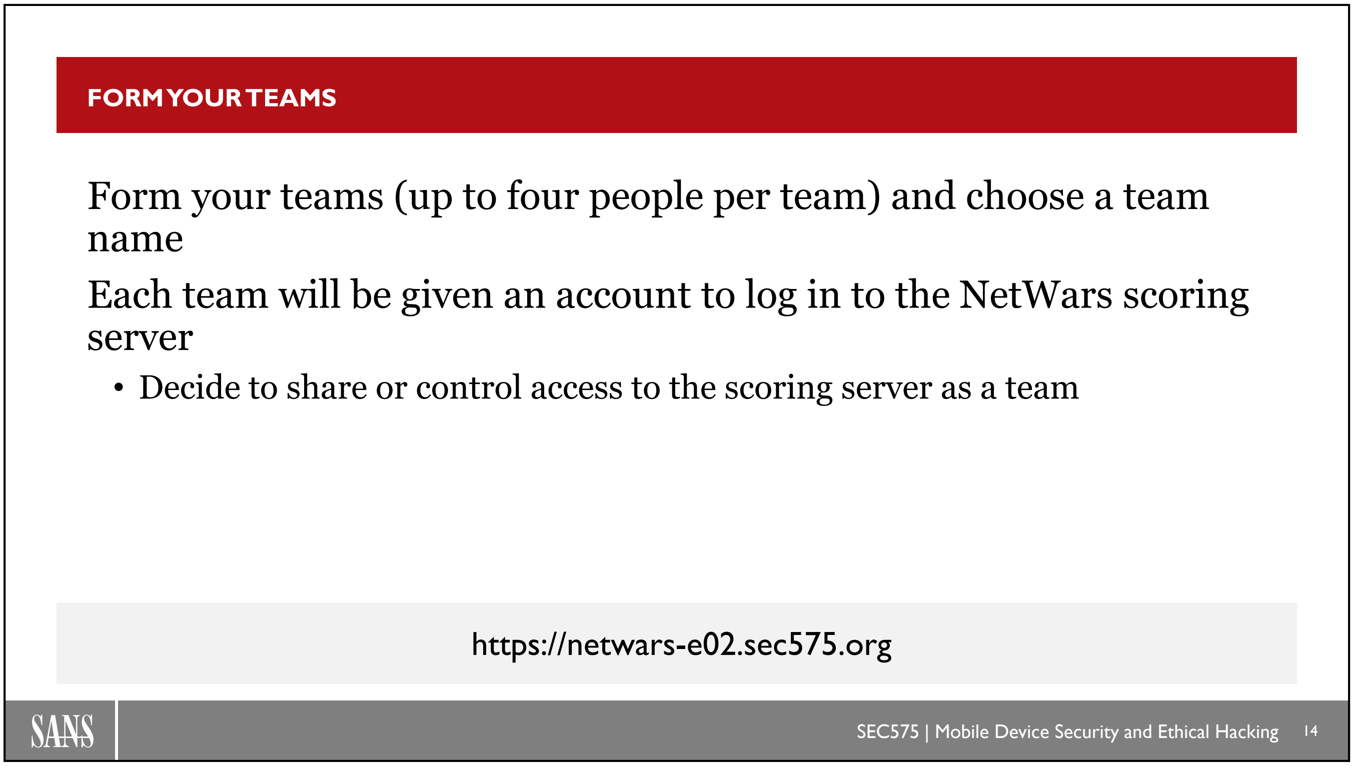
Winning

To win the SEC575 challenge, your team must be the first to achieve a score of 100 points (a perfect game) or be the highest scoring team at the end of the game.

In past challenges, some teams racked up points very quickly, but they might have lost a few points for wrong answers. Even when teams finish early, they are not automatic winners because teams who finish later with a higher score (closer to perfect) can be declared the winner.

Be careful about answering questions too quickly because this can easily lead to point loss. To avoid costly mistakes, confer with your teammates to validate your answers before you submit them.

© SANS Institute 2019



FORM YOUR TEAMS

Form your teams (up to four people per team) and choose a team name

Each team will be given an account to log in to the NetWars scoring server

- Decide to share or control access to the scoring server as a team

https://netwars-e02.sec575.org

SANS

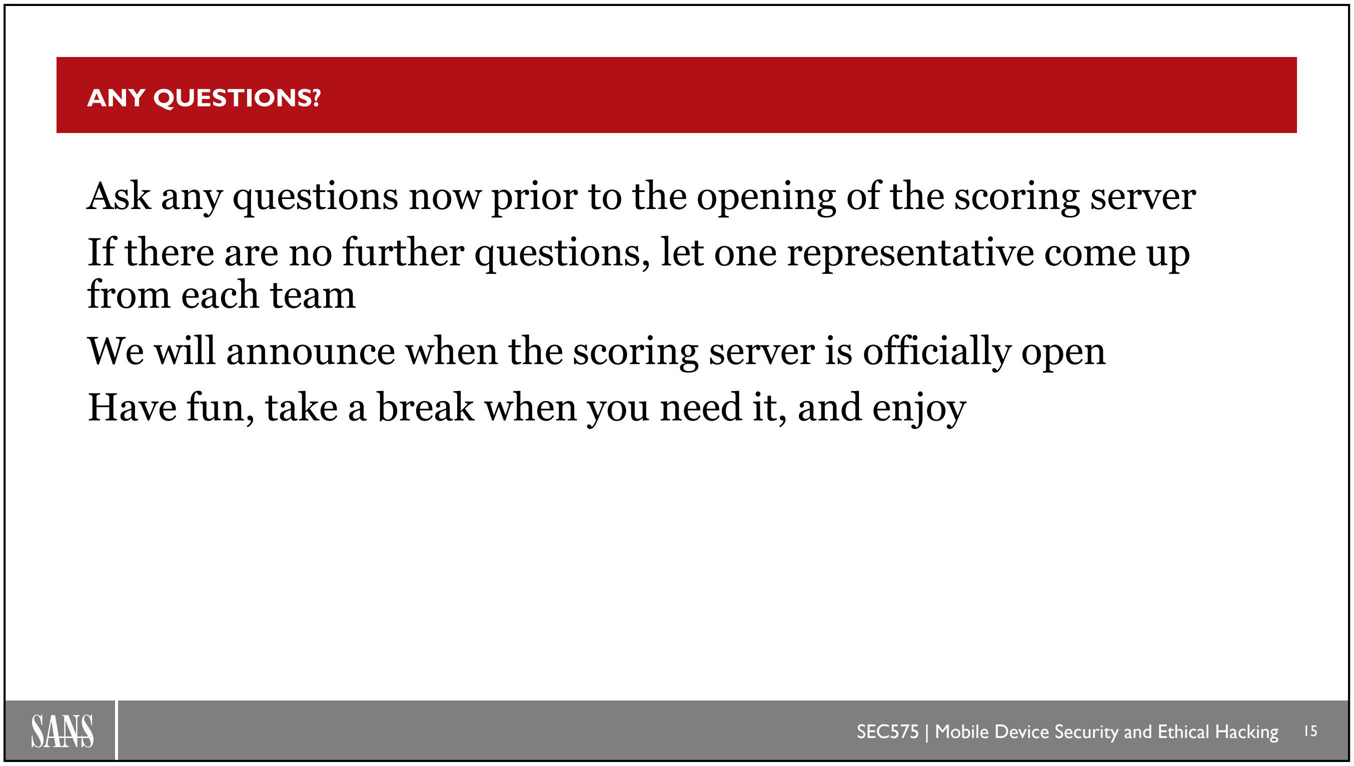
SEC575 | Mobile Device Security and Ethical Hacking 14

Form Your Teams

In a minute, you will be asked to form your teams (no more than five people per team) and choose a PG-appropriate team name. Each team will be given an account to log in to the NetWars scoring server at the URL on this page.

As a team, decide whether you will share the login credentials for the scoring server with the team or appoint one person who is responsible for submitting answers and distributing analysis tasks.

© SANS Institute 2019



ANY QUESTIONS?

Ask any questions now prior to the opening of the scoring server

If there are no further questions, let one representative come up from each team

We will announce when the scoring server is officially open

Have fun, take a break when you need it, and enjoy

SEC575 | Mobile Device Security and Ethical Hacking 15

Any Questions?

At this point, ask any questions prior to the opening of the scoring server. Once the question and answer phase is done, one representative from each team should see the instructor for credentials to the scoring server while the rest of the team prepares its systems for analysis. We will make an announcement when the scoring server is officially open.

During the workshop, have fun and enjoy. If you need to take a break, get a beverage or a snack; if you need to walk around and think for a few minutes, please feel free, but be respectful of the other teams and do not disturb their analysis work.

© SANS Institute 2019

This page intentionally left blank.

© SANS Institute 2019

Index

© SANS Institute 2019

© SANS Institute 2019

© SANS Institute 2019

© SANS Institute 2019

© SANS Institute 2019

© SANS Institute 2019

© SANS Institute 2019

© SANS Institute 2019

© SANS Institute 2019

© SANS Institute 2019

© SANS Institute 2019