SANS

www.sans.org

SECURITY 511

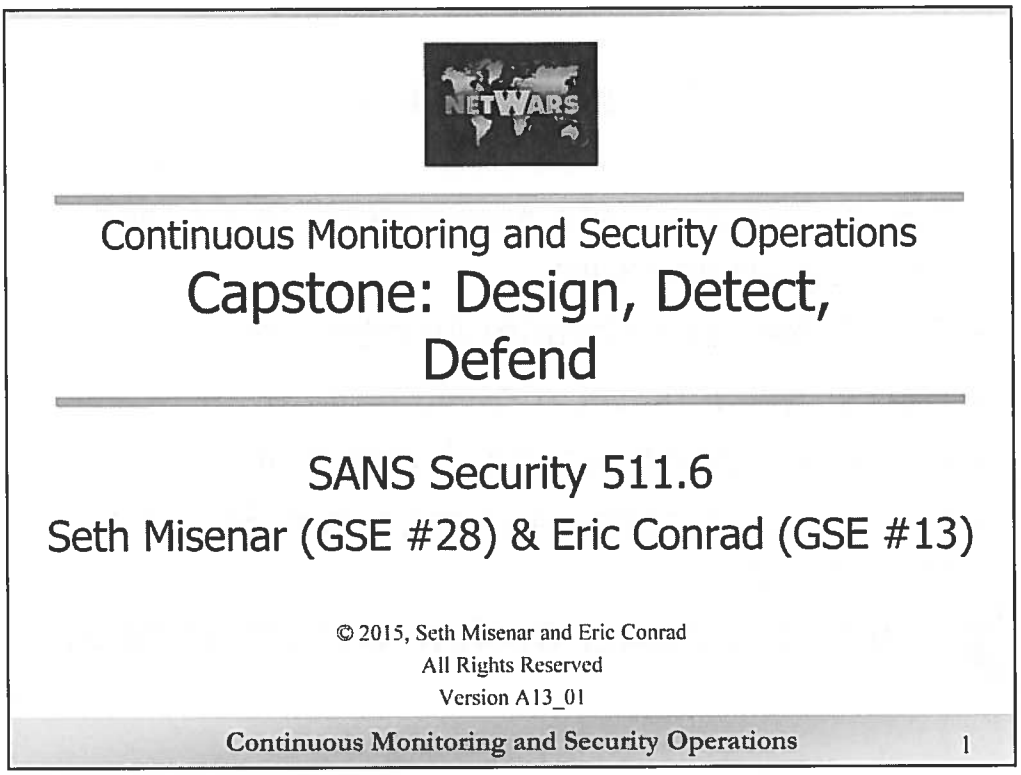
CONTINUOUS MONITORING AND SECURITY OPERATIONS

511.6

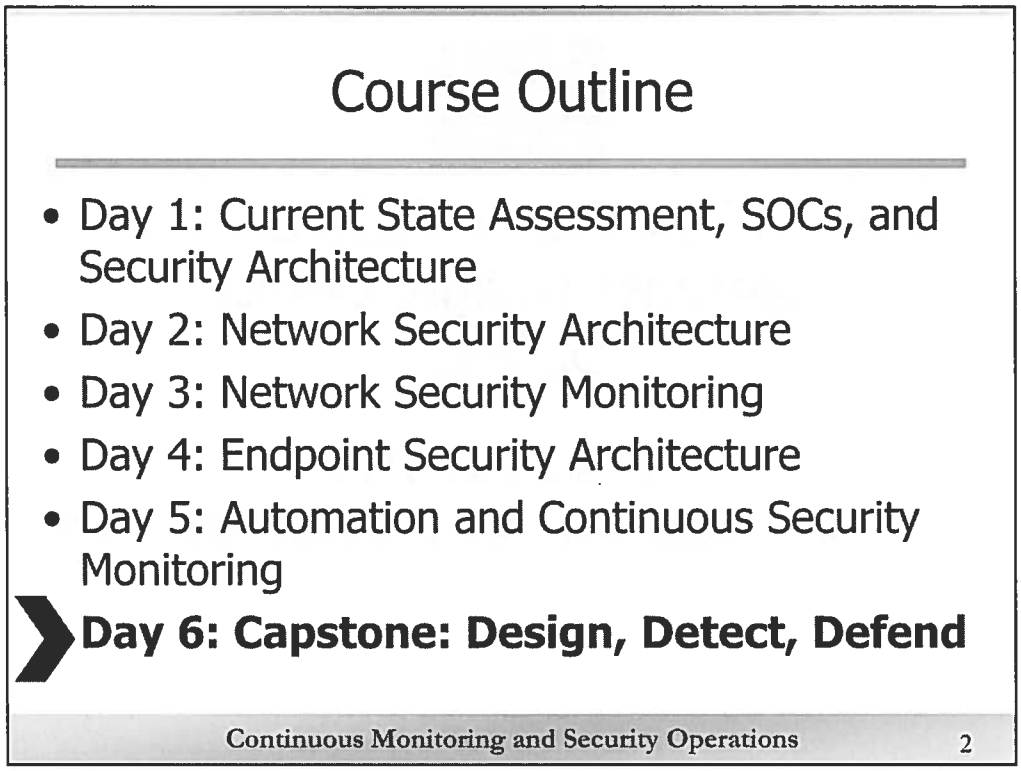
Capstone: Design, Detect, Defend

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

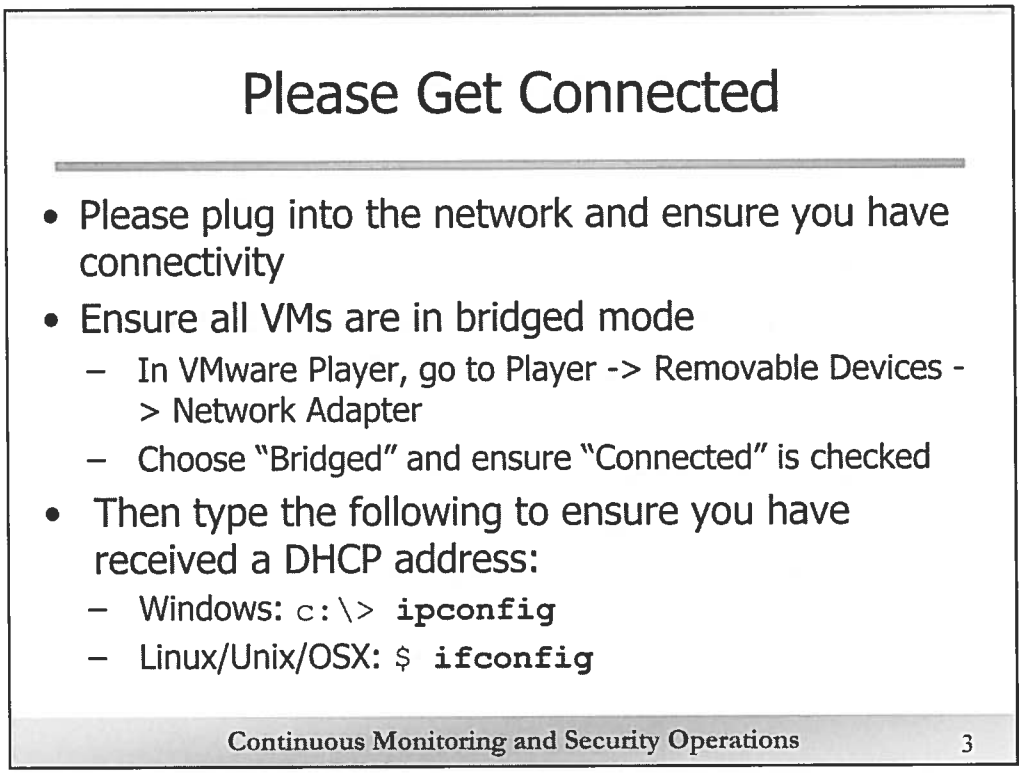
Sec511_6_A13_01



Welcome to SANS Security 511.6, Capstone: Design, Detect, Defend!



Next up: the Design, Detect, and Defend capstone!



Please ensure that the cat5 cable you're using has tabs both ends. These often break off, leading to layer 1 problems during the exercise.

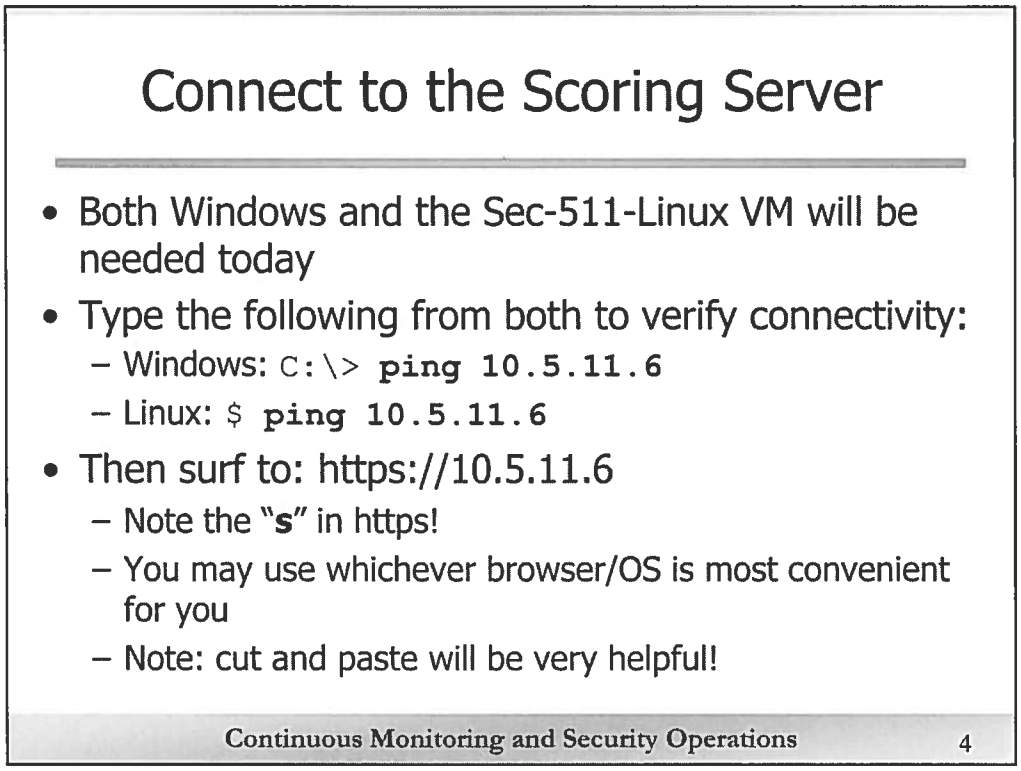
Also, ensure that your Ethernet port's link light is on.

You should receive a DHCP address on the 10.5.100.0/23 subnet.

If you would like to use one or more static addresses: please use 10.5.102.X, and ask your instructor for "X" (your last octet). You may then also use 10.5.103.X, 10.5.104.X, etc. Also: ensure your netmask is 255.255.0.0!

Note: if you have VMware Workstation, you may configure bridged networking by going to: VM -> Removable Devices -> Network Adapter -> Settings

In VMware Fusion, it is: Virtual Machine -> Network Adapter -> Settings



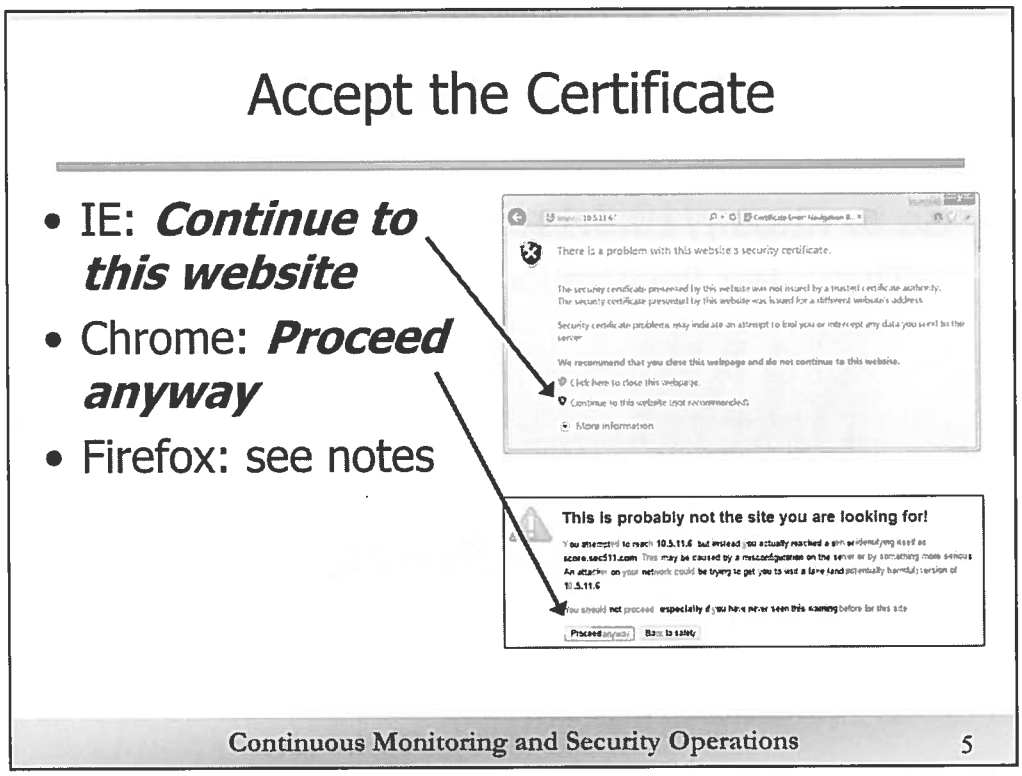
Please ping from both Linux and Windows to verify connectivity to the scoring server:

```
$ ping 10.5.11.6
```

```
C:\> ping 10.5.11.6
```

The ability to cut and paste will be *quite* useful as you enter flags into the scoring server.

The Sec-511-Linux VM has VMware tools installed, and should support cut and paste. Please test cutting and pasting between Windows and Linux to verify.



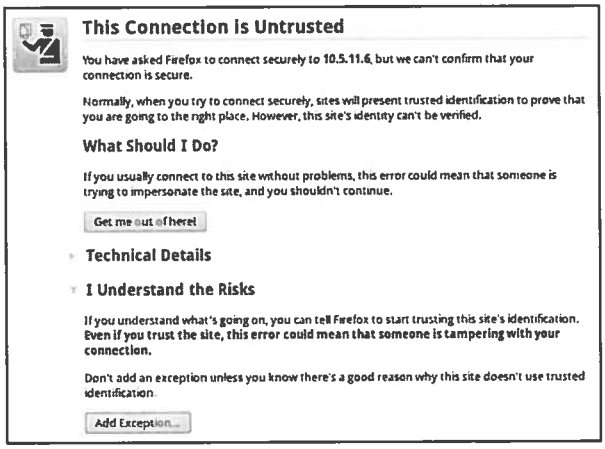
The scoring server is also available at https://score.sec511.com (and has a public DNS entry). Any host or VM with Internet access will be able to resolve score.sec511.com and access the server via the name.

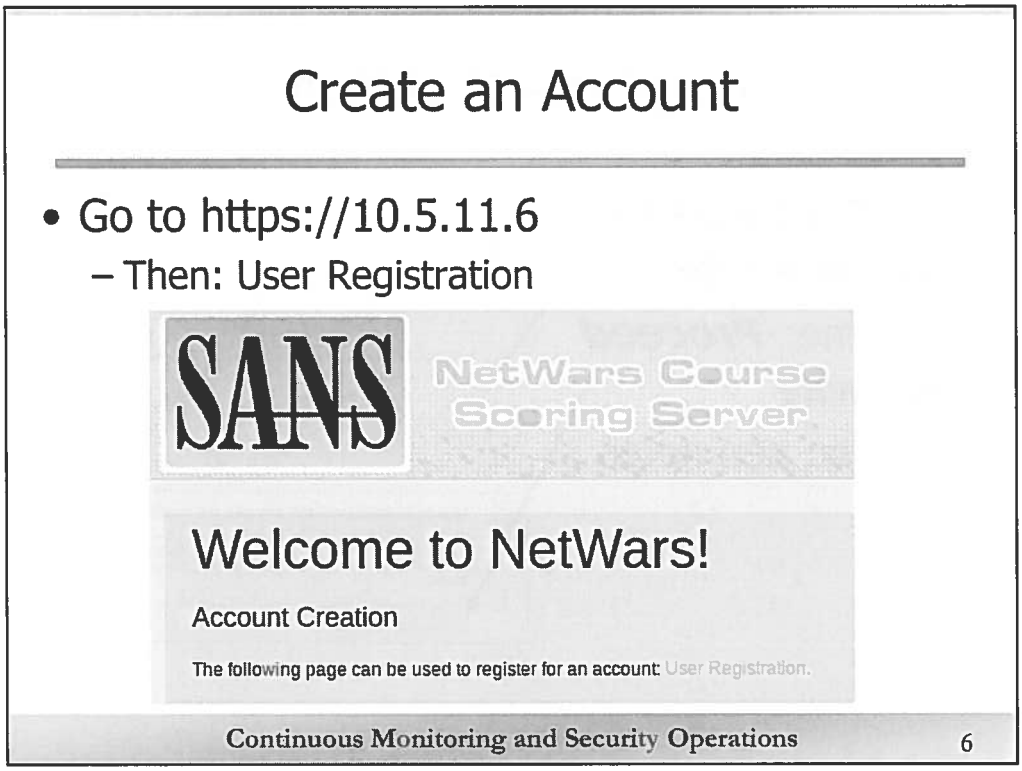
The Linux VM has this entry in its /etc/hosts file, so you may access https://score.sec511.com from Linux, and will not receive a certificate warning.

Your Windows host or VM will not have the hosts file entry, so it will be simplest to use the scoring server's IP address directly: https://10.5.11.6.

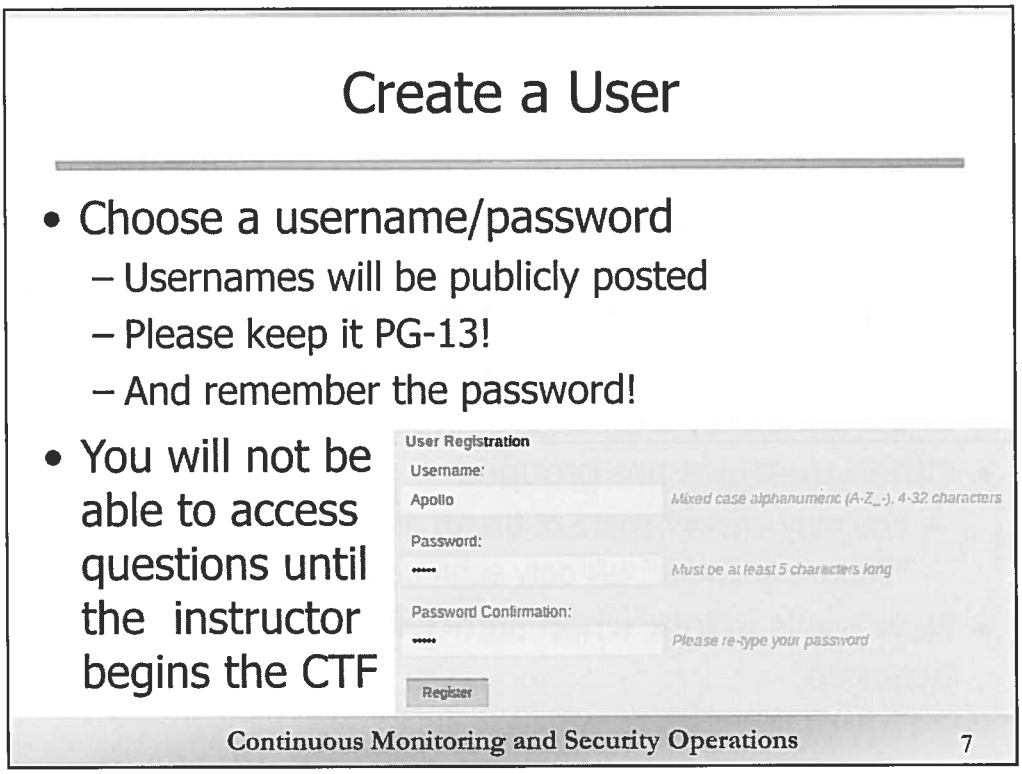
Firefox requires three steps:

1. *I understand the risks*
2. *Add Exception*
3. *Confirm Exception*





You should now see the NetWars Scoring Server. Please click on "User Registration."



Choose a username and password.

Your username will be posted on the leaderboard, so please keep it professional.

Also: please choose a good password, and remember it.

You will not be able to access questions until the instructor starts the game. At that point all accounts will be able to access the CTF.

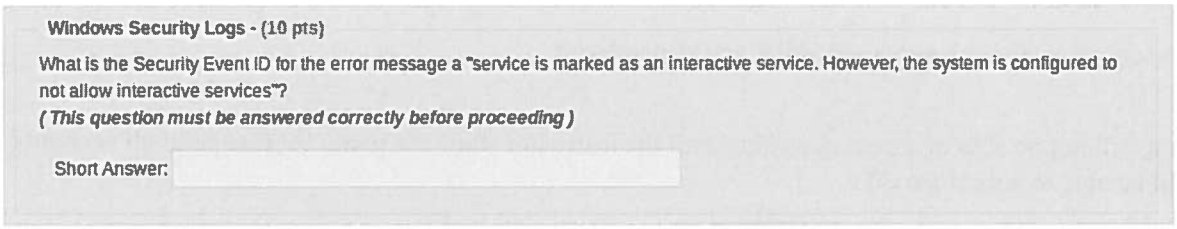
Game Design

- There are multiple levels
  - And multiple "missions" per level
  - You may attempt missions in any order
- Some questions are gateway questions
  - Correct answer unlocks more questions
- Other questions are grouped
  - You may answer some of these, and leave others blank
  - "Submit Answers" will only submit answered questions
- New levels unlock when sufficient points have been acquired

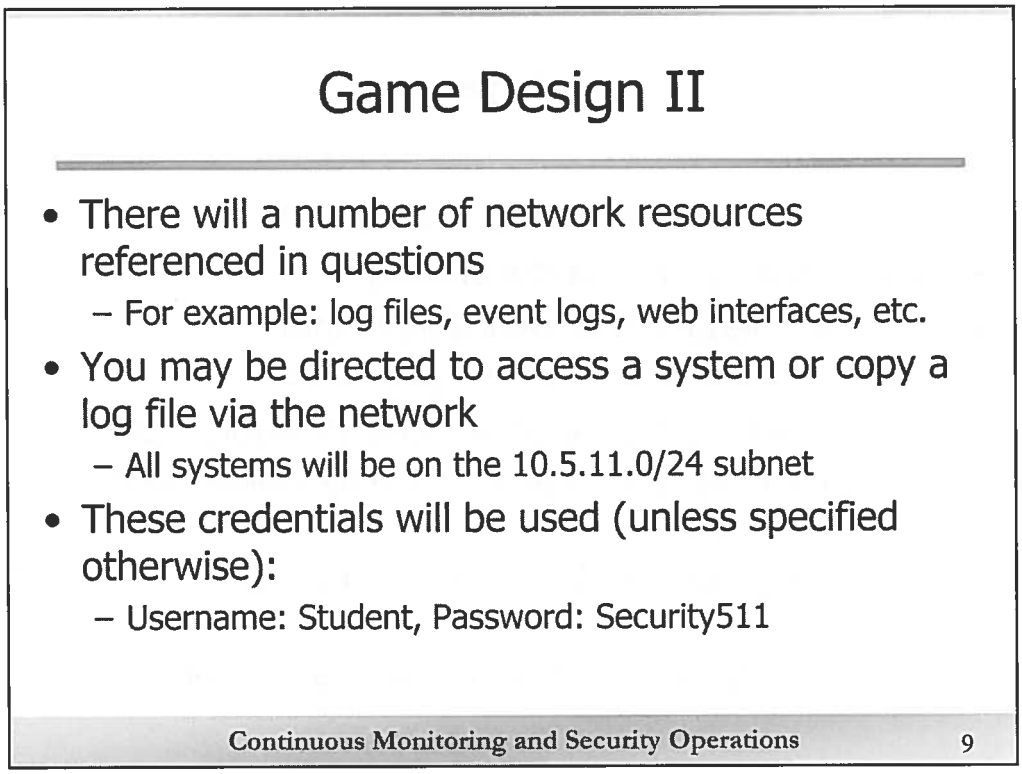
Continuous Monitoring and Security Operations 8

Gateway questions will have the following text:

(This question must be answered correctly before proceeding)



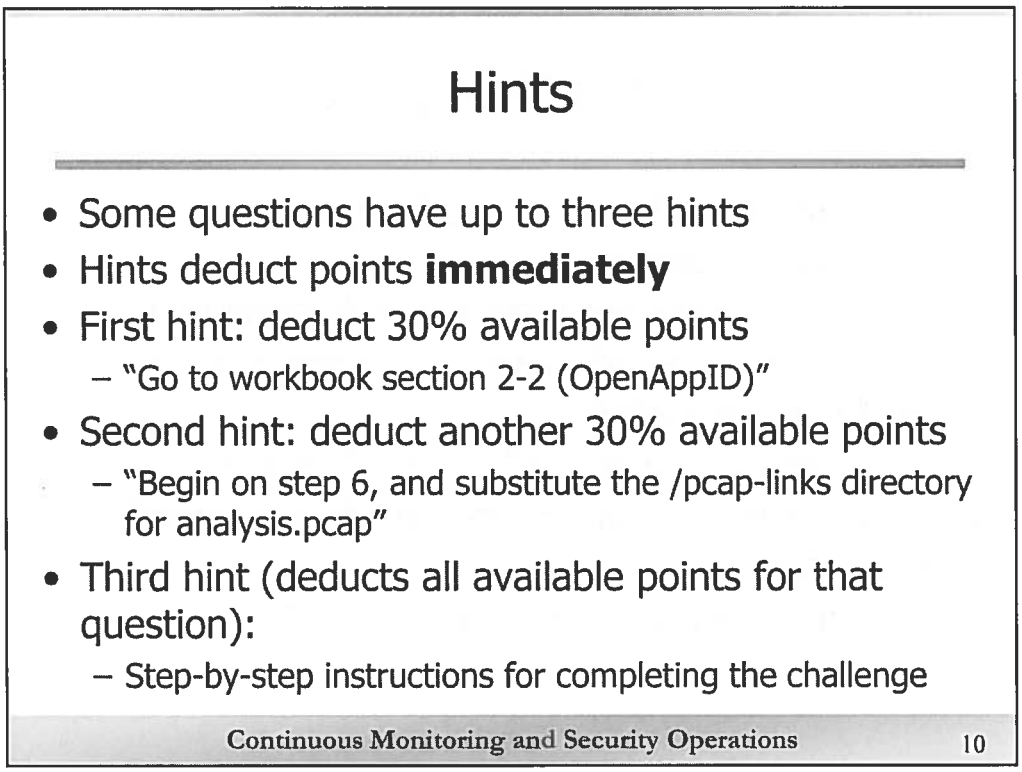
More questions will unlock once the gateway question is answered correctly.



The network you will be accessing is 10.5.11.0/24. In other words, every system you access will begin with 10.5.11.*, such as the score server at 10.5.11.6.

The credentials will be the same you use to access the Sec511-Linux-VM, unless otherwise indicated. If a domain is needed to access a Windows system, use SEC511.

If a network resource is required to answer a question, the question will give specific directions. For example: "Use scp to copy a log file from student@10.5.11.25:example.txt"

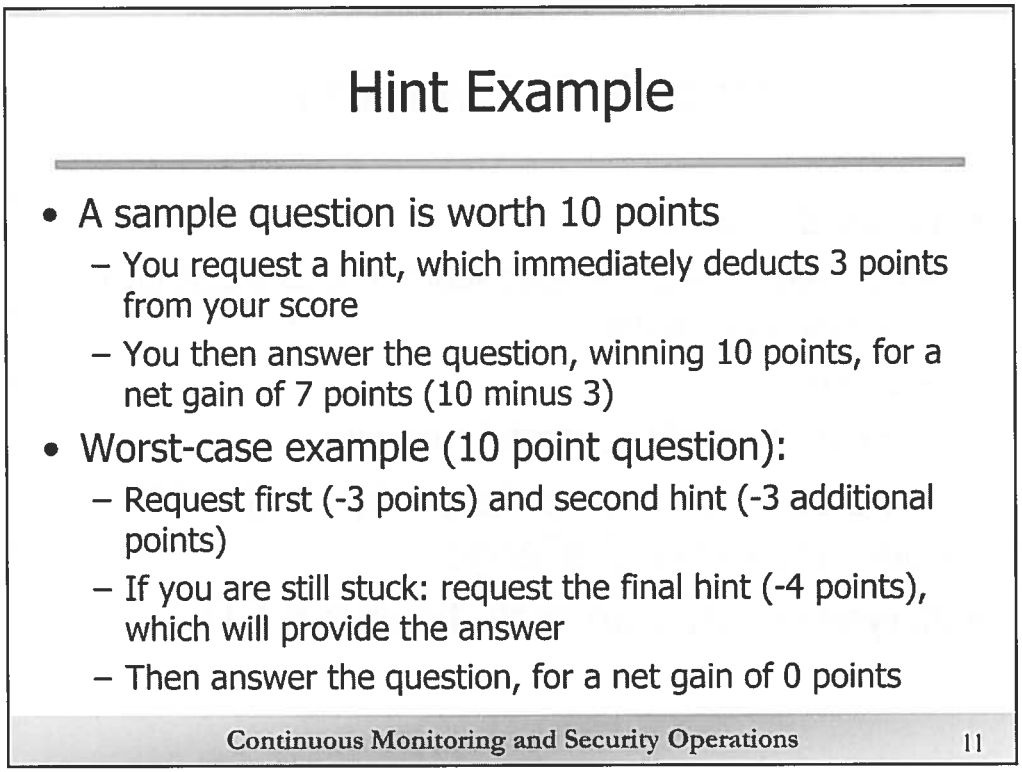


Hints are available for many questions. You can use hints in a number of ways. Remember the CTF is designed for learning and/or competing to win. You don't have to do both!

Please keep this in mind: points are deducted immediately!

One way to use hints is strategically: 70% of something is better than zero percent. If you can't answer a question, a hint can provide the necessary boost. The time saved may be critical.

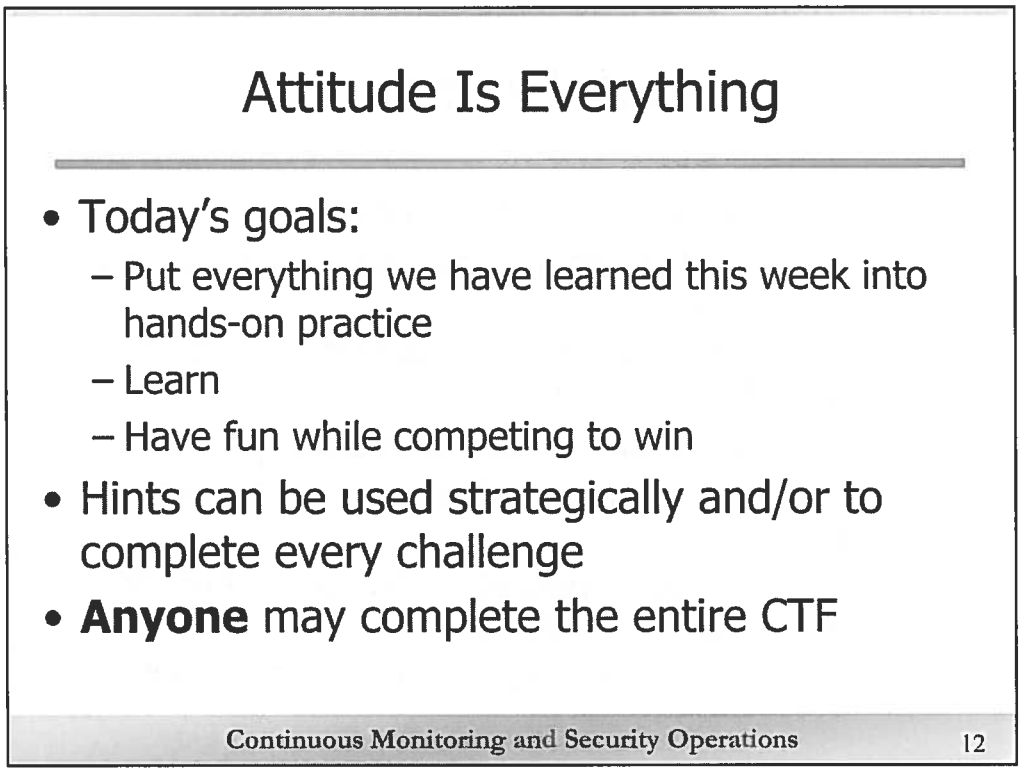
The other way to use hints is to complete steps you may be unable to complete otherwise. You can use hints to complete the entire CTF this way: the final hint is the answer.



Once you request a hint for a specific question: it is best to see it through to the end. Assuming a 10-point question, the first hit will deduct 3 points immediately. If you stop there, you will simply be down 3 points.

If you cannot answer the question after the first hint, request the second. Another 30% of question points will be deducted immediately, making you negative 6 points for a 10-point question.

If you still cannot answer the question, request the third hint, which will immediately deduct the final 40% of available points. You will be down 10 points on a 10-point question. Then answer the question winning 10 points, for a net gain of zero points.



Attitude Is Everything

We designed the NetWars capstone to be enjoyable for all: from management to the hands-on experienced hunt teamer with years of experience in the trenches.

Hints are available at varying costs, from subtle nudge to "here's how you do it: type this…"

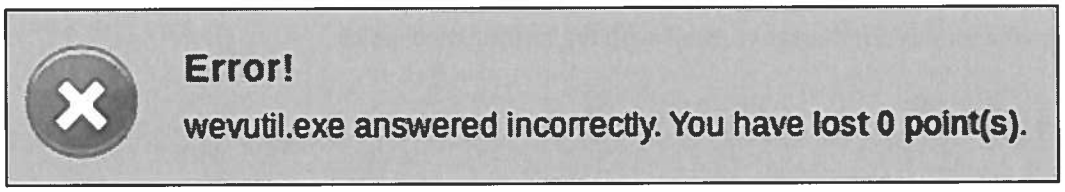
The capstone provides an opportunity to learn, and/or an opportunity to compete. You may choose the "no hints" method to maximize points, the "more hints" method to maximize learning, or a combination of the two methods.

How it Works

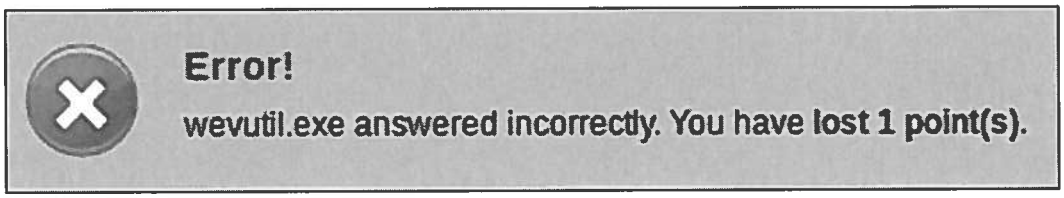
- There is no penalty for one wrong answer to a question
- After that, each wrong answer deducts a point from your total
- This is done to
  - Encourage high quality work
  - Discourage blind guessing, brute forcing, etc.

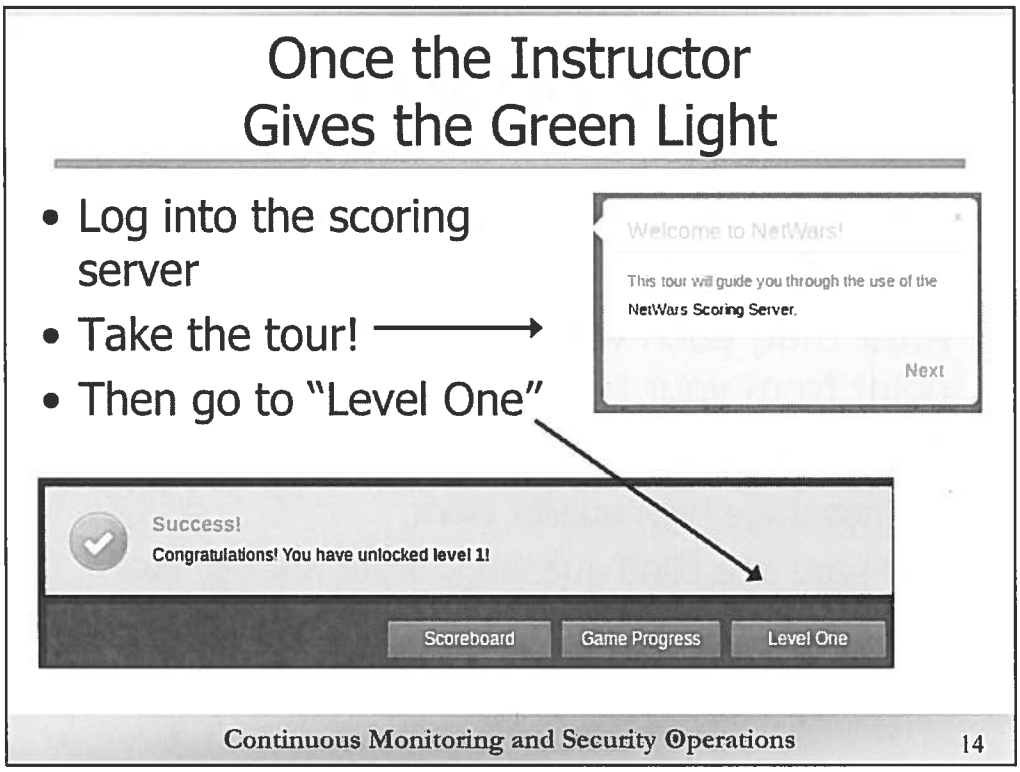
Continuous Monitoring and Security Operations 13

There is no penalty for one wrong answer to a question:



There is a one-point penalty for each incorrect answer after the first:

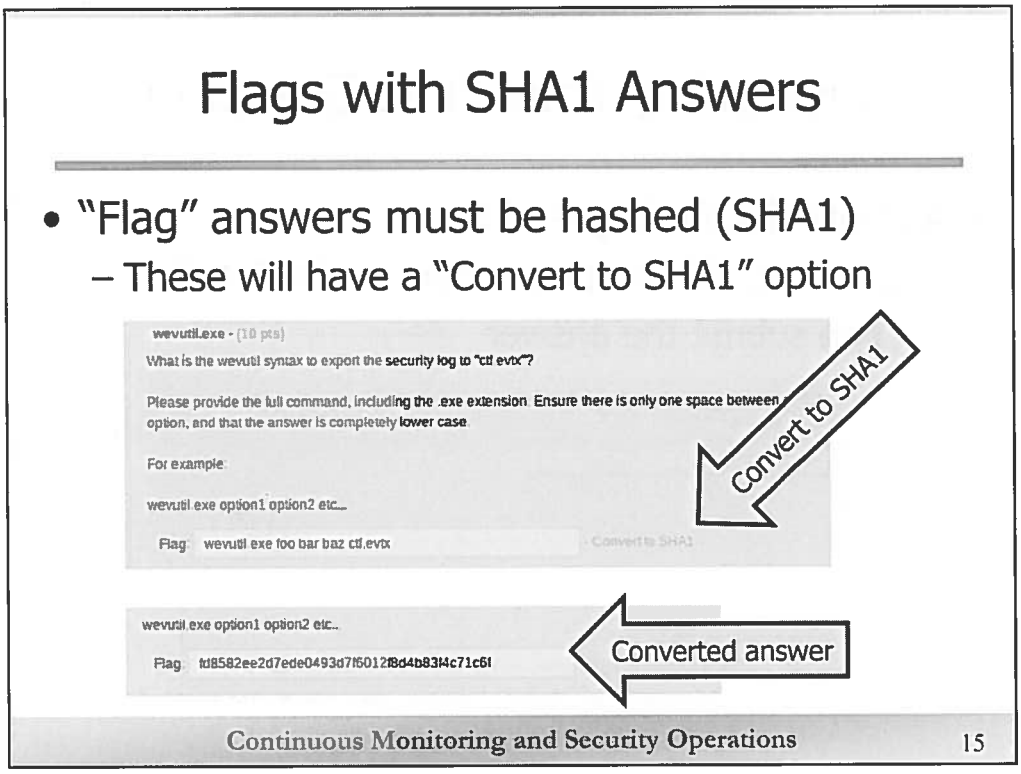




Level one will unlock once the instructor begins the game.

You may take the tour to familiarize yourself with the scoring mechanics.

Then go to "Level One."

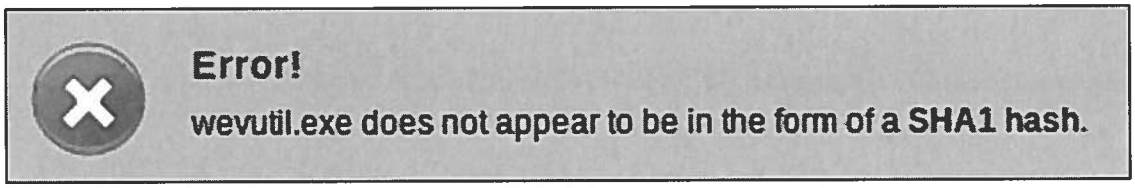


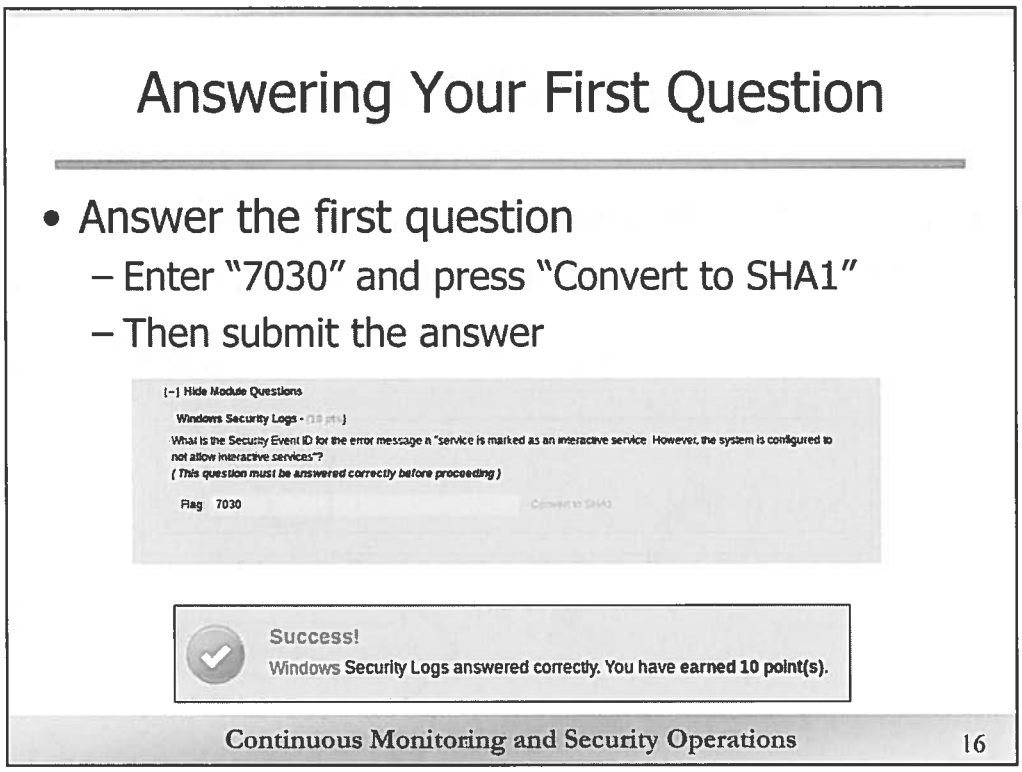
Hashed answers will always have a "Convert to SHA1" link on the right, which will automatically hash the string entered in the Flag:" box.

Be very careful with case and spaces with SHA1 answers! A change of a single character will make the answer incorrect. The question will specify case when necessary (for example: Windows commands).

You will need to provide the correct case when you should be able to determine it. For example: Linux is case sensitive, and Linux commands are usually lower case.

The server will generate the error you see below if you enter something that is not a SHA1 hash in a flag question that requires a SHA1 answer. There is no penalty for this error.





The first question is:

> What is the Security Event ID for the error message a "service is marked as an interactive service. However, the system is configured to not allow interactive services"?

This is a flag question, with a SHA1 hash answer.

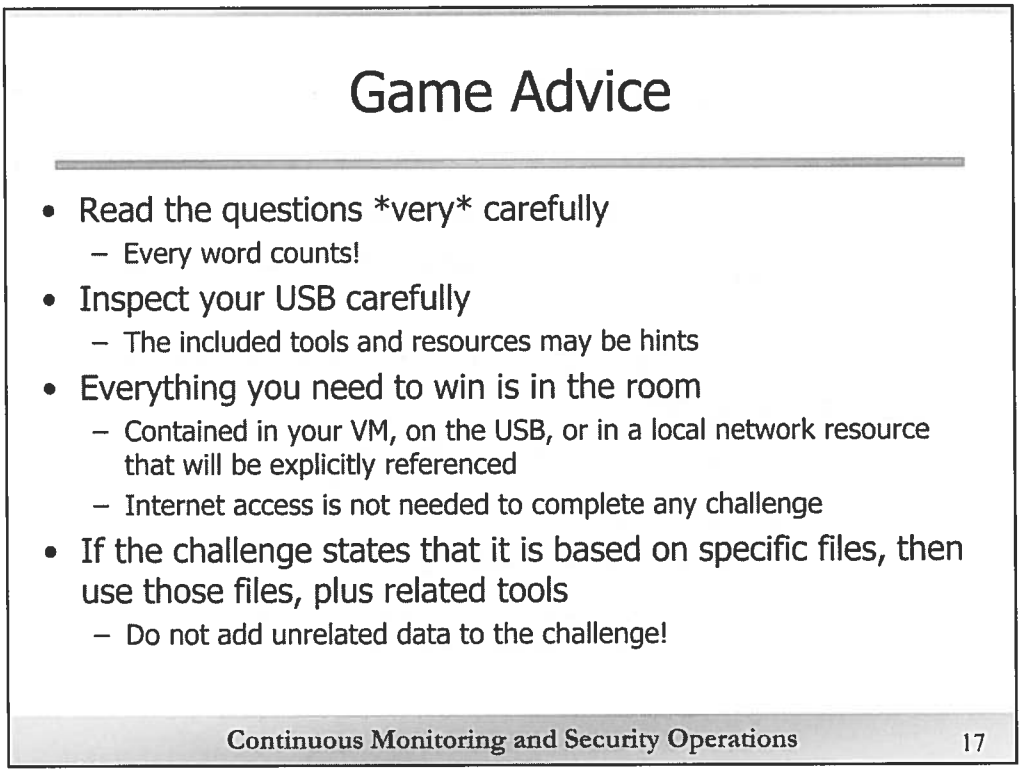
We're being generous and giving you the first answer: 7030. Enter that, and press "Convert to SHA1." Then press "Submit Answers".

Yay, points!

It will become more difficult shortly, we promise!

We discussed event 7030 during the 511.5 section *Critical Event 1: Service Creation*

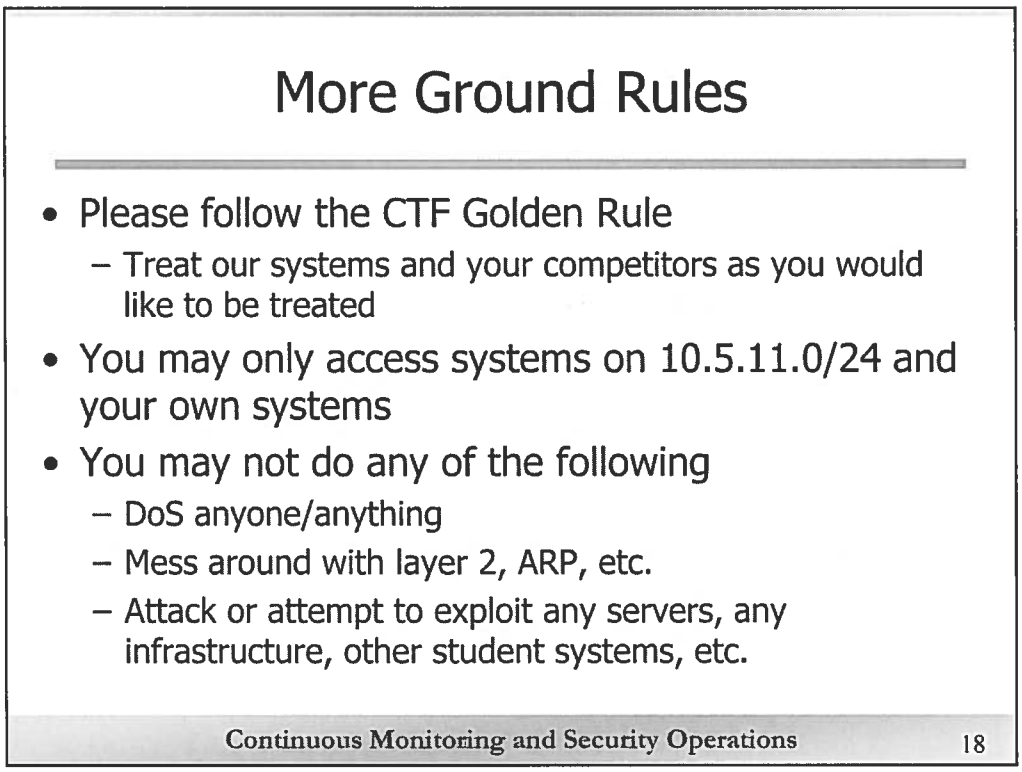
> Sysinternals PsExec generates no errors, but Metasploit's generates Event ID 7030
>
> > *The MIehTND service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.*



It may go without saying: but **read the questions carefully**! Students often lose points due to carelessness.

Your USB contains a few files that are hints, check it out.

Most of the challenges are based directly on previous labs. If you are stuck: flip through the lab workbook. This is one of the reasons we placed all of the labs in a dedicated book.

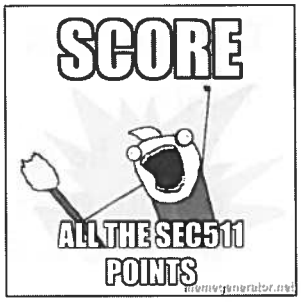


Please play according to the rules: they are designed to ensure maximum learning and enjoyment for everyone!

The instructor reserves the right to dismiss any student who does not comply with their rules.

Declaring a Winner

- We will play until roughly 2:00 PM
  - Assuming a 9:00 AM start time
- The winner is the player who either
  - Scores all the points
  - Has the most points when the game ends
- The instructor will then recap the game



Continuous Monitoring and Security Operations 19

Today will be a lot more free-flowing than days 1 through 5. You may take breaks or lunch whenever you'd like.

The game will last roughly 5 hours, or 9 AM to 2:00 PM, assuming a normal conference start time.

Any Questions?

- The game is about to begin
  - If you have any last-minute questions: now is the time to ask
- We provided the first answer: 7030
- After that, it's up to you!

If you have any questions, please ask them now!

Otherwise, let the games begin!

[1] http://kidvskat.wikia.com/wiki/File:1-1_-_Let_The_Games_Begin.png

Index

Version A13_01

Please let us know if you find any errors in the index. Also, reach out if you have suggestions to improve the index (e.g. keywords that should be added, removed, or have page references added or removed). The easiest way to submit these improvements is to email 511@contextsecurity.com.

Seth Misenar and Eric Conrad