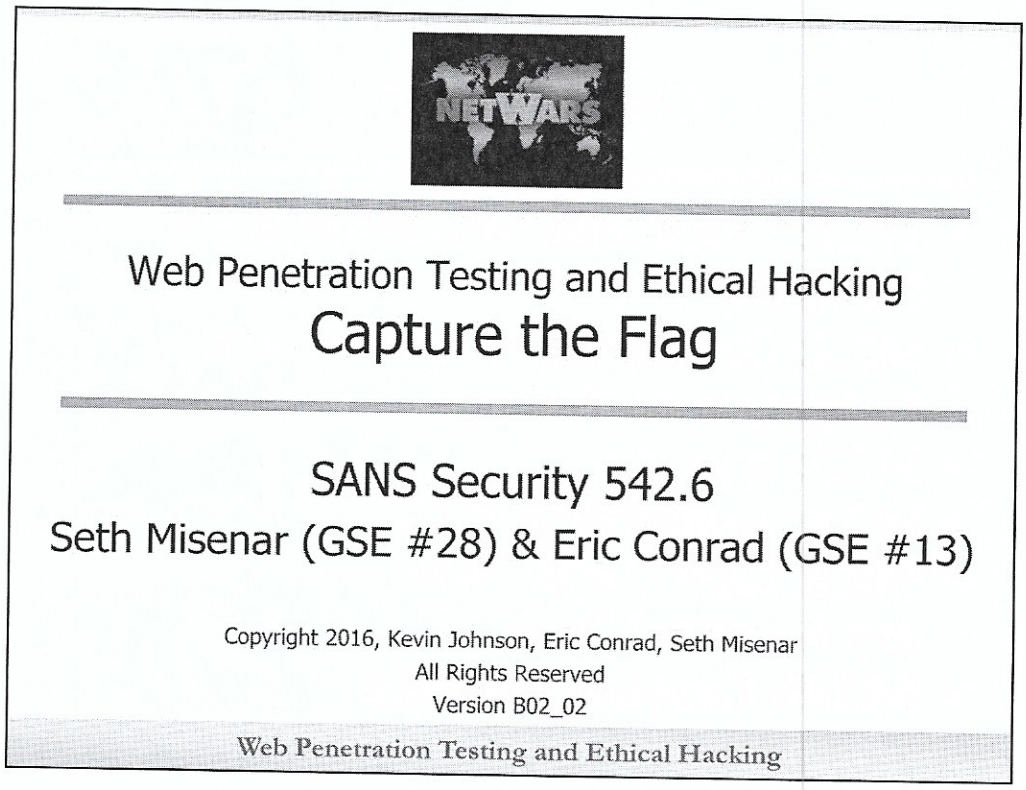
542.6
Capture the Flag

542.6
Capture the Flag



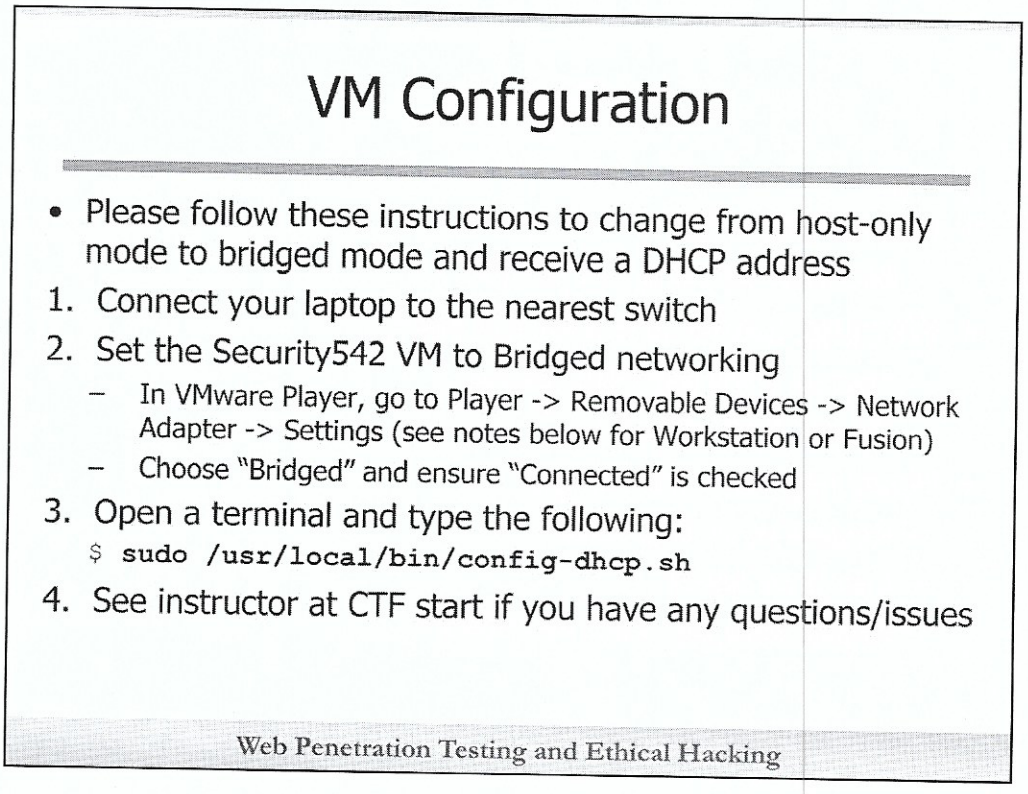
Welcome to the SANS Security 542.6. Today we will work within teams to perform a web application penetration test. This will be against an example set of web applications as are typically seen in corporate networks. We will use the methodology and tools we have covered over the last five days.

Course Outline

- 542.1: Introduction and Information Gathering
- 542.2: Configuration, Identity, and Authentication Testing
- 542.3: Injection
- 542.4: JavaScript and XSS
- 542.5: CSRF, Logic Flaws and Advanced Tools
- **542.6: Capture the Flag**

Web Penetration Testing and Ethical Hacking

Welcome to the Security 542 Capture the Flag exercise!



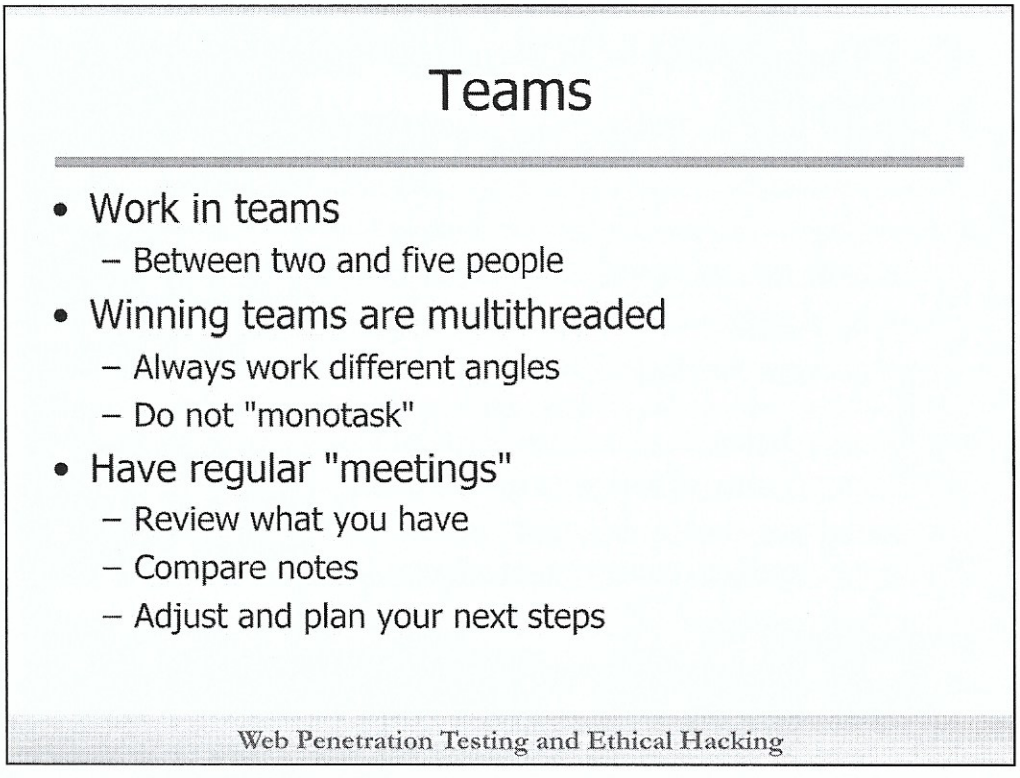
For the CTF we will be working on a live network. This requires some changes from the setup that has served us so well all week. Please be sure to complete the following steps to ensure you (and your team) have the best CTF experience possible.

1. Connect your laptop to the nearest switch
2. Change Security542 VM from Host Only to Bridged networking
   - In VMware Player, go to Player -> Removable Devices -> Network Adapter -> Settings
     - See below for Workstation or Fusion
   - Choose "Bridged" and ensure "Connected" is checked
3. Open a terminal and type the following:

   ```
   $ sudo /usr/local/bin/config-dhcp.sh
   ```
4. See instructor at CTF start if you have any questions/issues

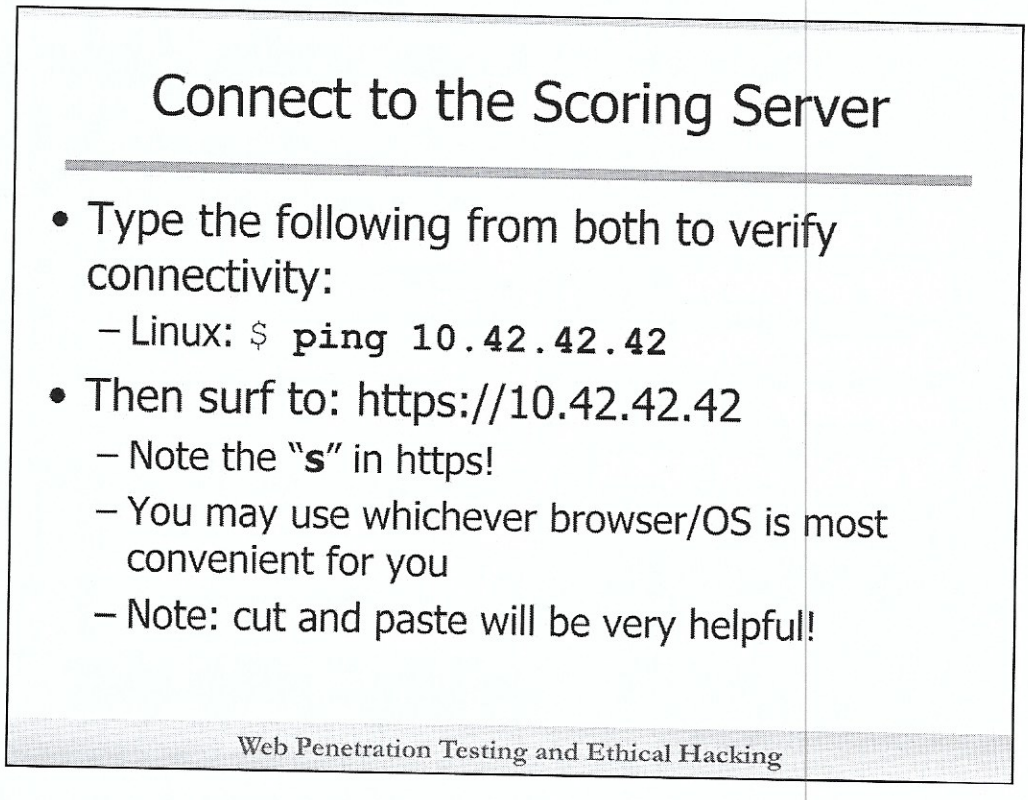
Note: if you have VMware Workstation, you may configure bridged networking by going to: VM -> Removable Devices -> Network Adapter -> Settings

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



Please 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 five. We find that more than five becomes overkill in this environment. People start getting left out.

Have each person record their findings and steps. But make sure that you have regular meetings to compare notes and make sure that you are working together. This is VERY important.

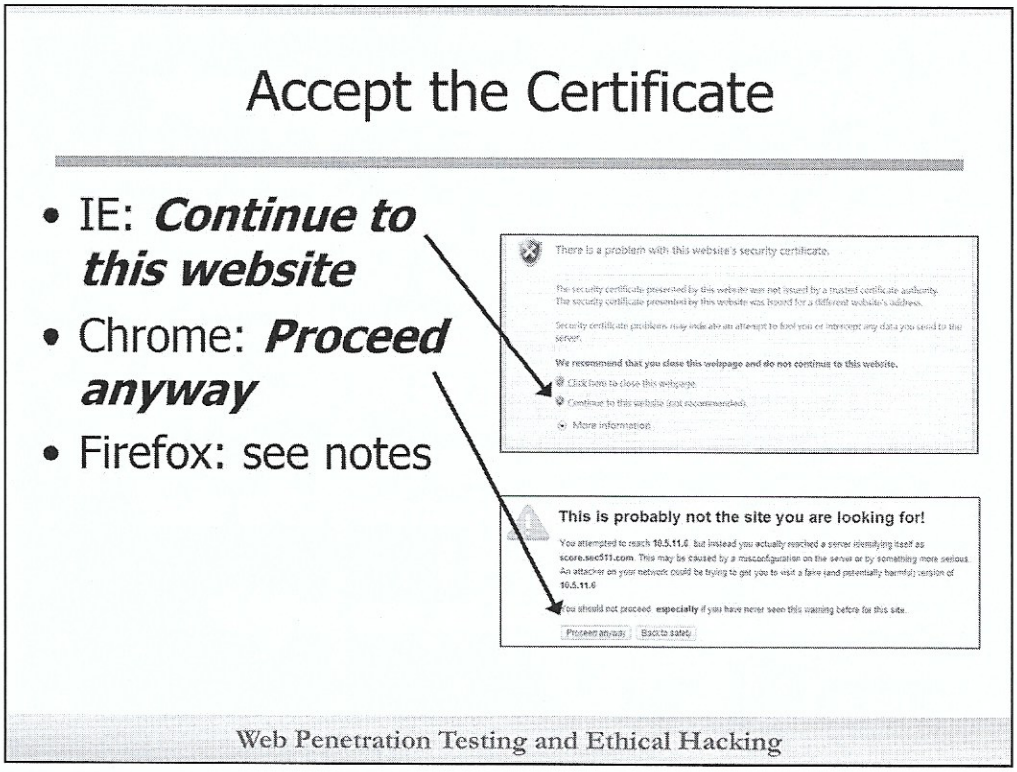


Please ping from both your Sec542 Linux VM and your host to verify connectivity to the scoring server:

```
$ ping 10.42.42.42
```

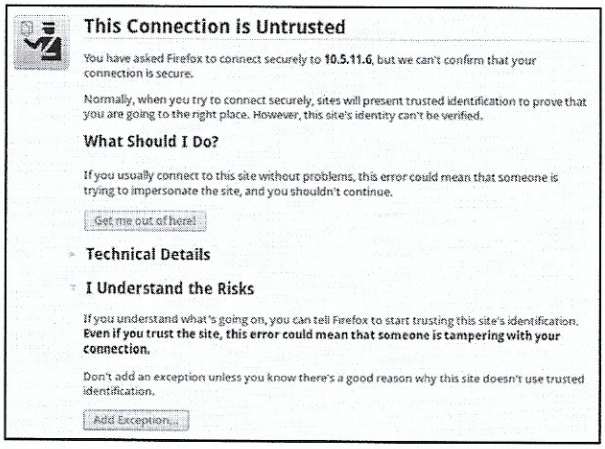
```
C:\> ping 10.42.42.42
```

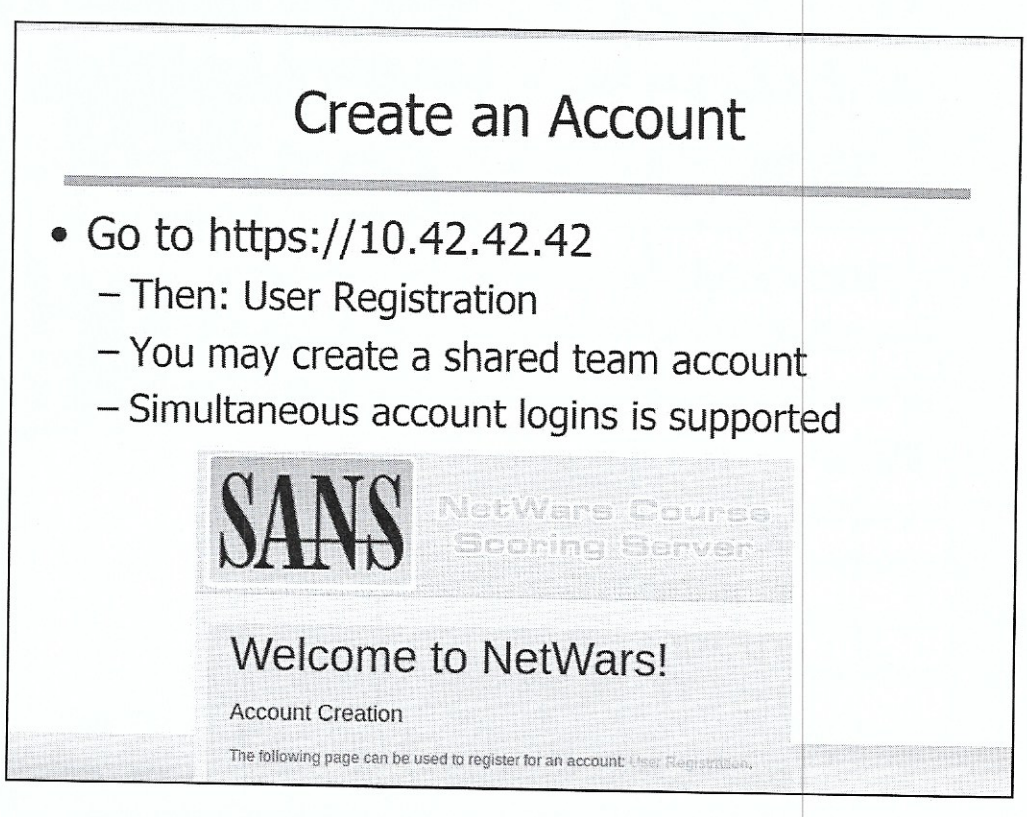
The ability to cut and paste will be *quite* useful as you enter flags into the scoring server.



Firefox requires three steps:

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

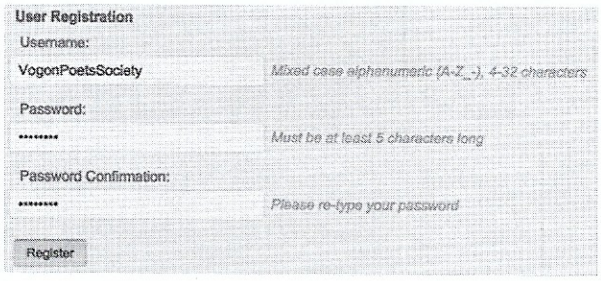




You should now see the NetWars Scoring Server. Please click on "User Registration."

Create a User

- Choose a team username/password
  - Usernames will be publicly posted
  - Please keep it PG-13!
  - And remember the password!
- You will not be able to access questions until the instructor begins the CTF



Web Penetration Testing and Ethical Hacking

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.

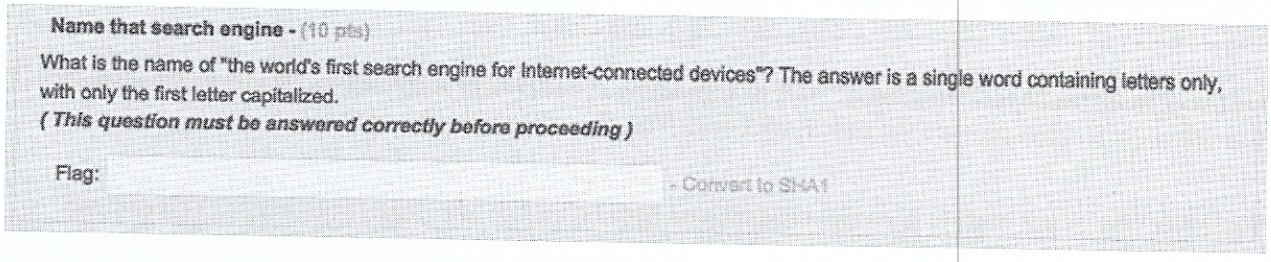
Game Design

- 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

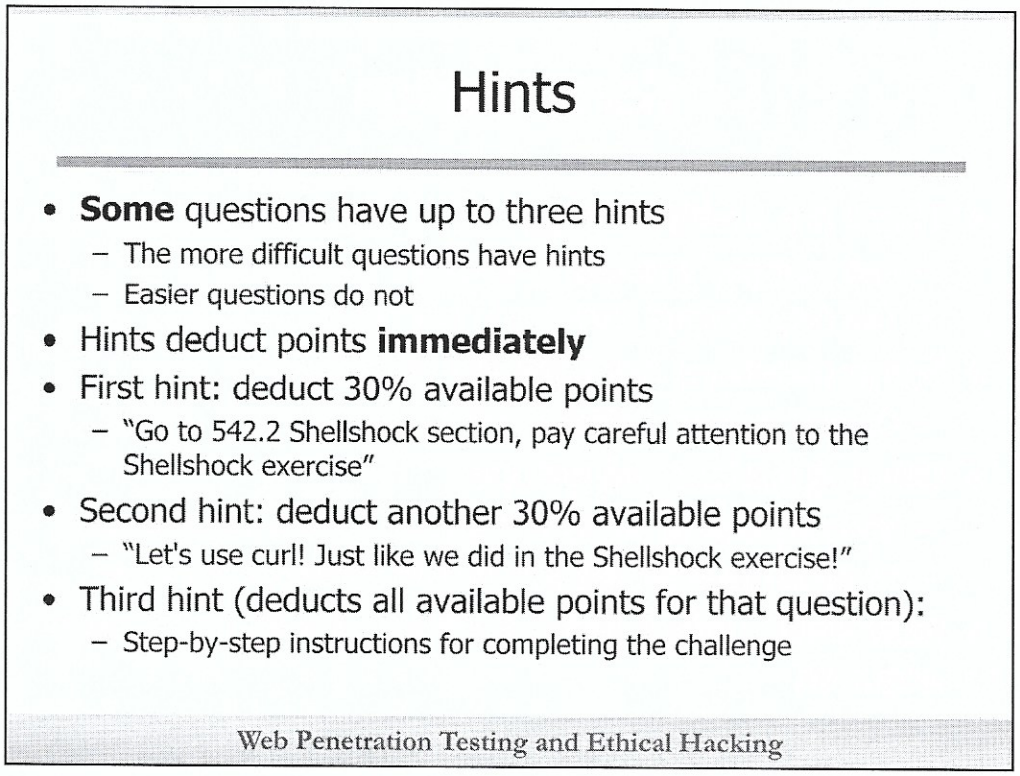
Web Penetration Testing and Ethical Hacking

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.

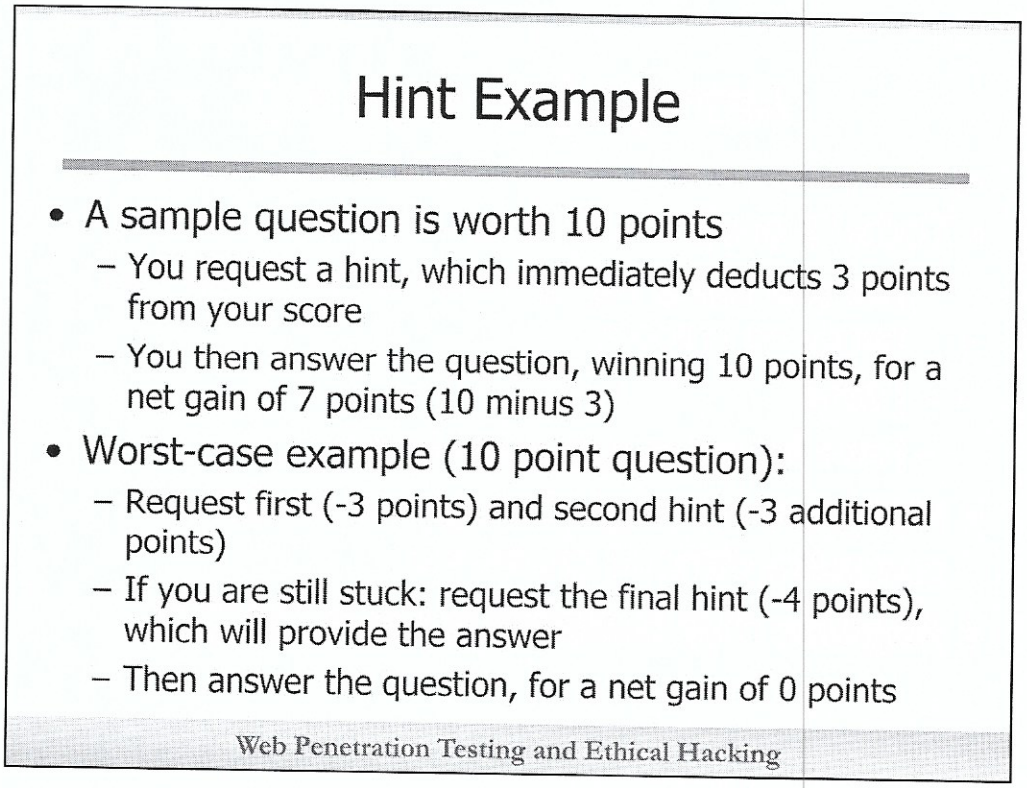


Hints are available for many questions. You can use hints in a number of ways. Remember the CTF is designed for learning and/or competing to win. You don't have to do both!

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.

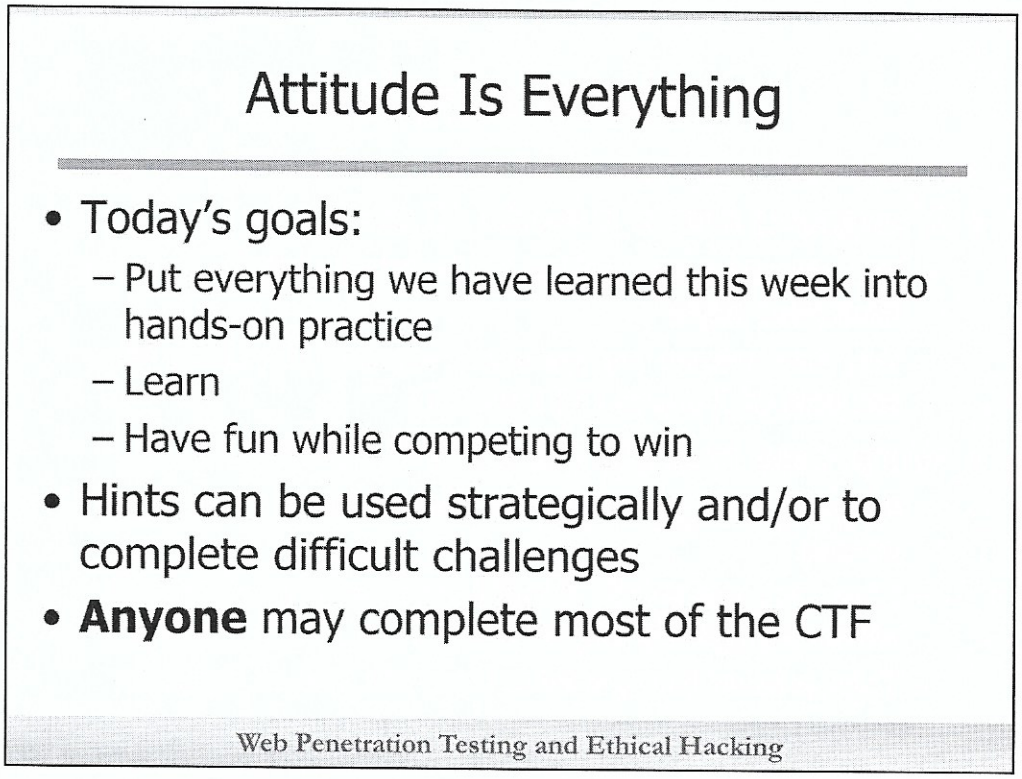
The other way to use hints is to complete steps you may be unable to complete otherwise. You can use hints to complete the entire CTF this way: the final hint is the answer.



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 penetration tester with years of experience in the trenches.

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

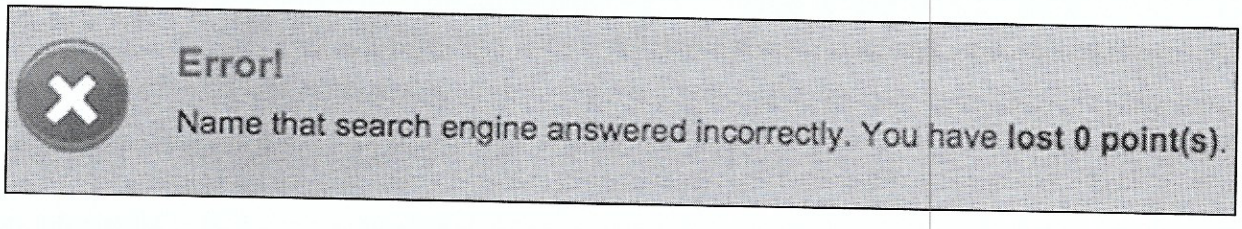
The capstone provides an opportunity to learn, and/or an opportunity to compete. You may choose the "no hints" method to maximize points, the "more hints" method to maximize learning, or a combination of the two methods.

How It Works

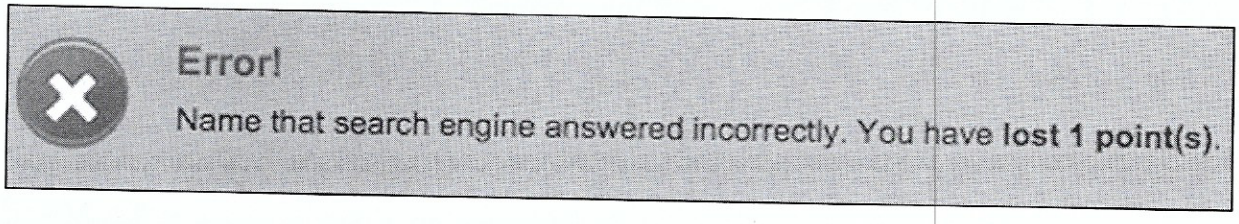
- There is no penalty for one wrong answer to a question
- After that, each wrong answer deducts a point from your total
- This is done to
  - Encourage high quality work
  - Discourage blind guessing, brute forcing, etc.
- **Do not** reload the page immediately after a wrong answer
  - Some browsers will auto-resubmit old (bad) answers!

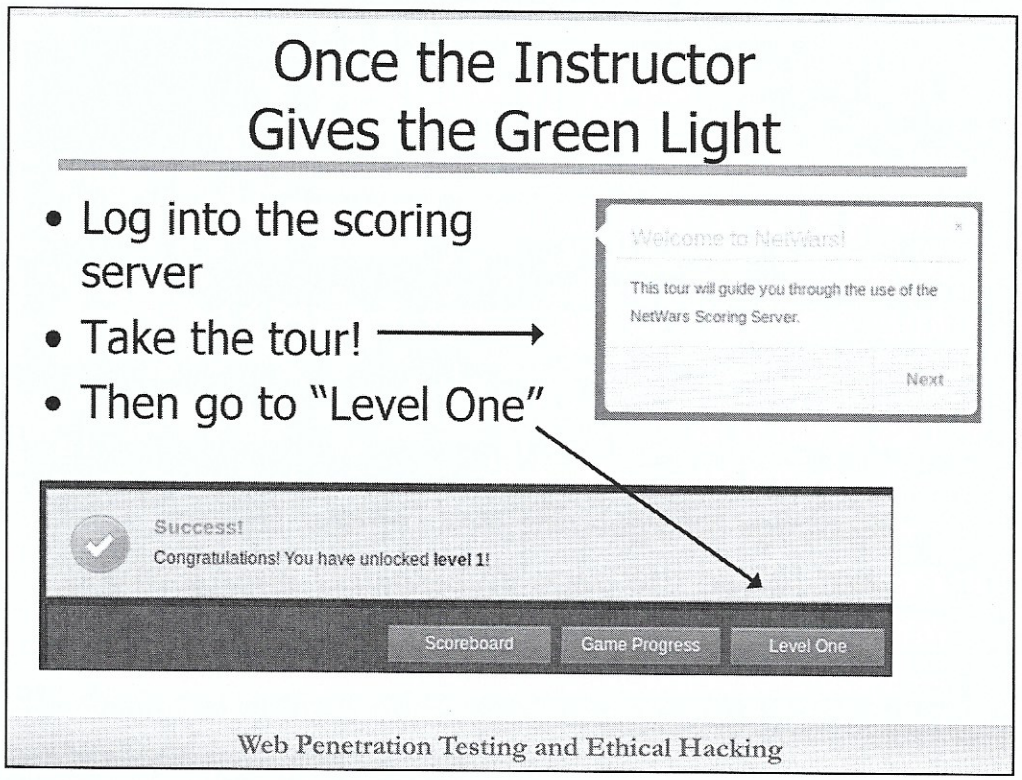
Web Penetration Testing and Ethical Hacking

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



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

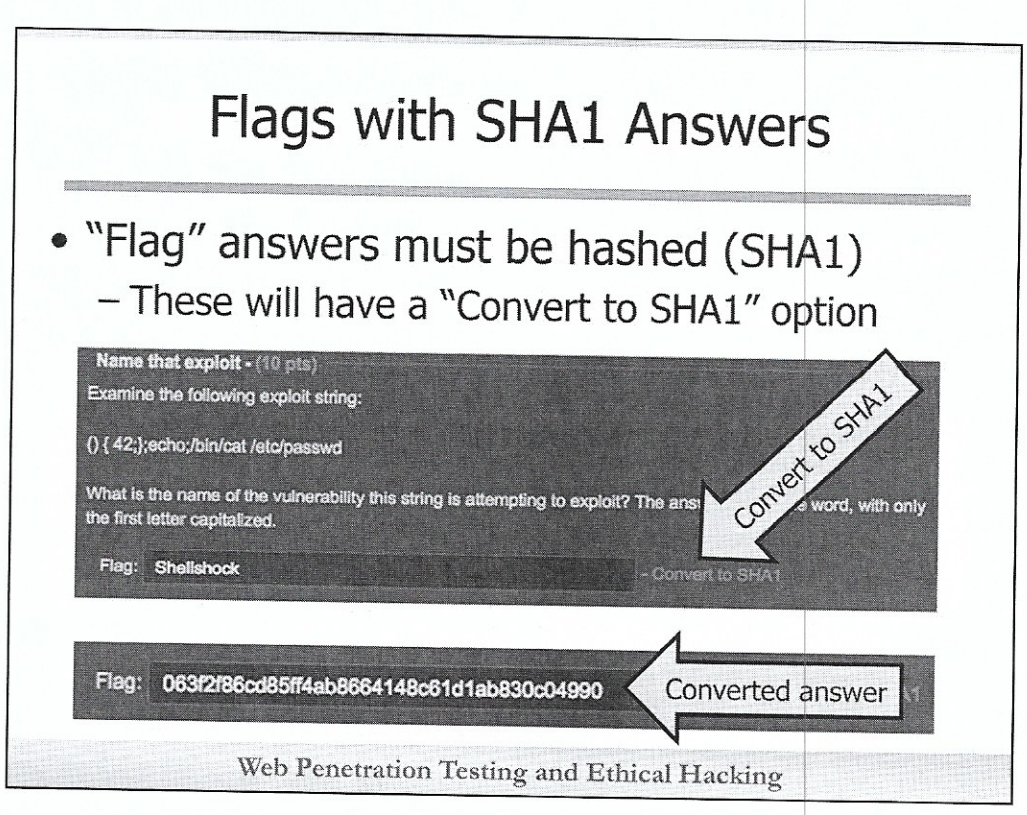




Level one will unlock once the instructor begins the game.

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

Then go to "Level One."

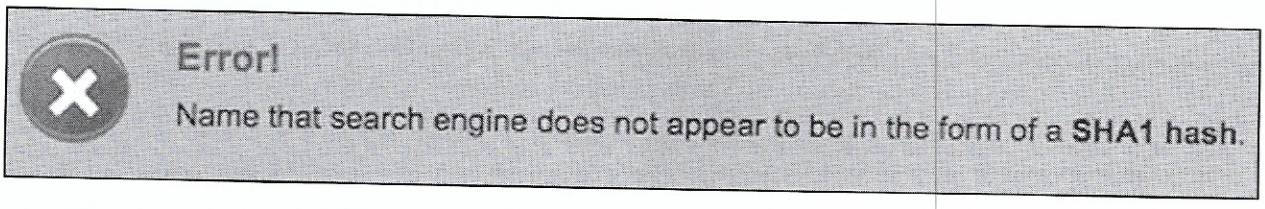


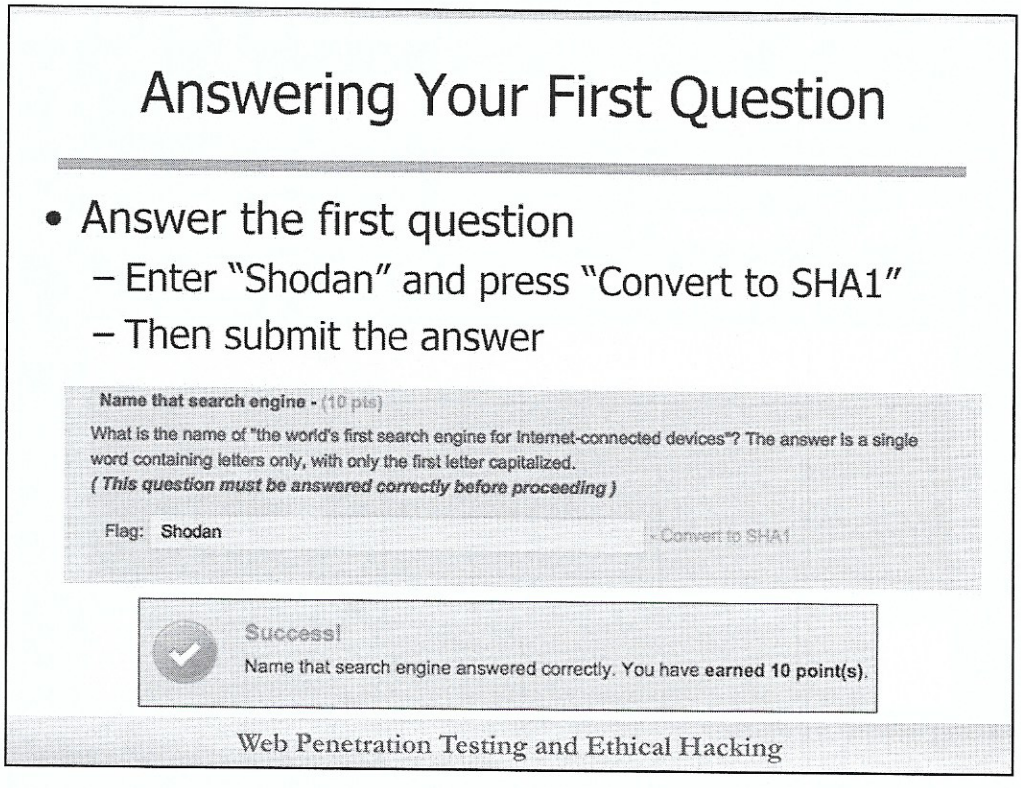
Hashed answers will always have a "Convert to SHA1" link on the right, which will automatically hash the string entered in the Flag:" box.

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:

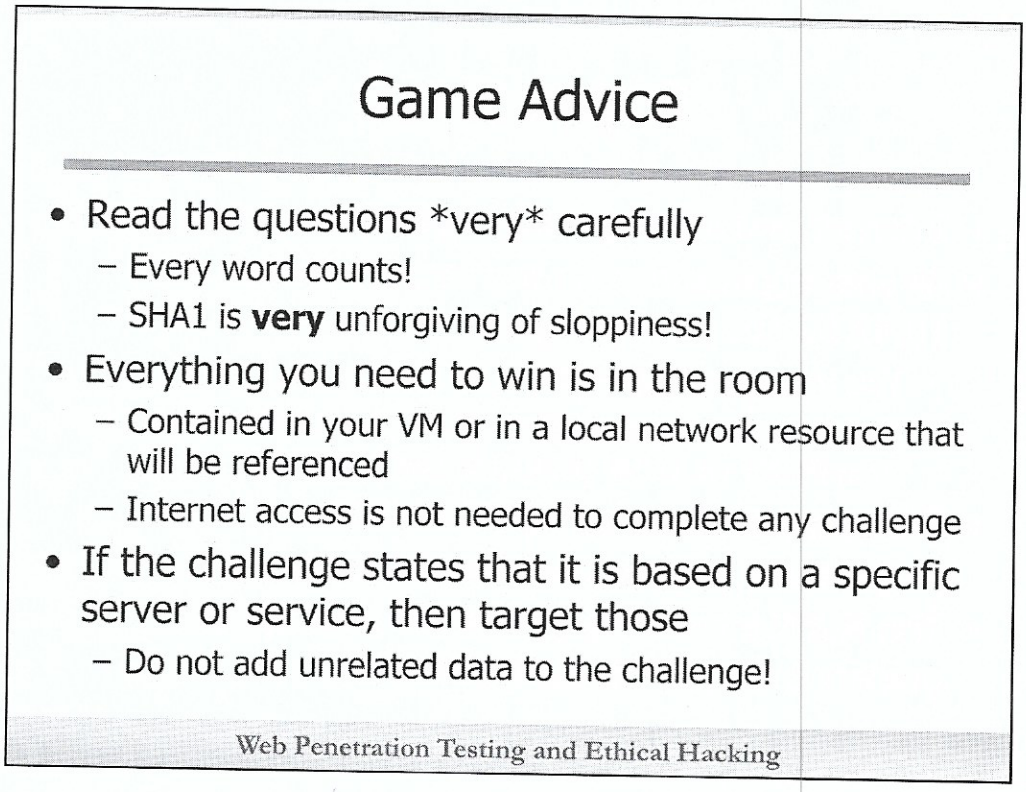
> What is the name of "the world's first search engine for Internet-connected devices"? The answer is a single word containing letters only, with only the first letter capitalized.

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

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

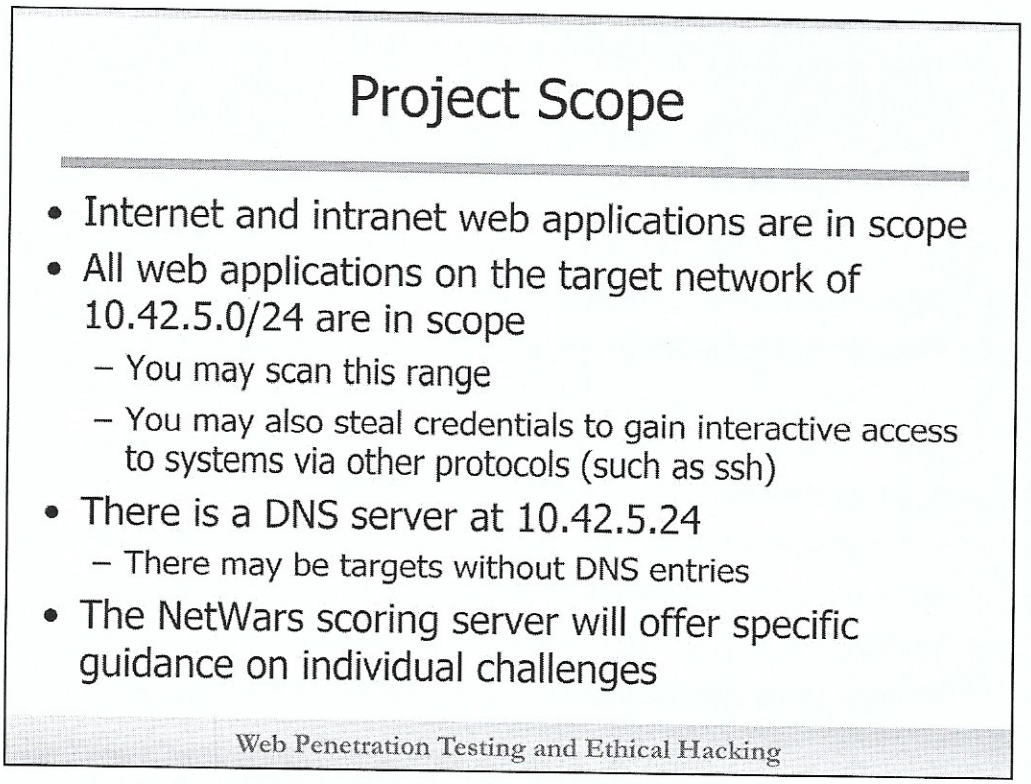
Yay, points!

It will become more difficult shortly, we promise!



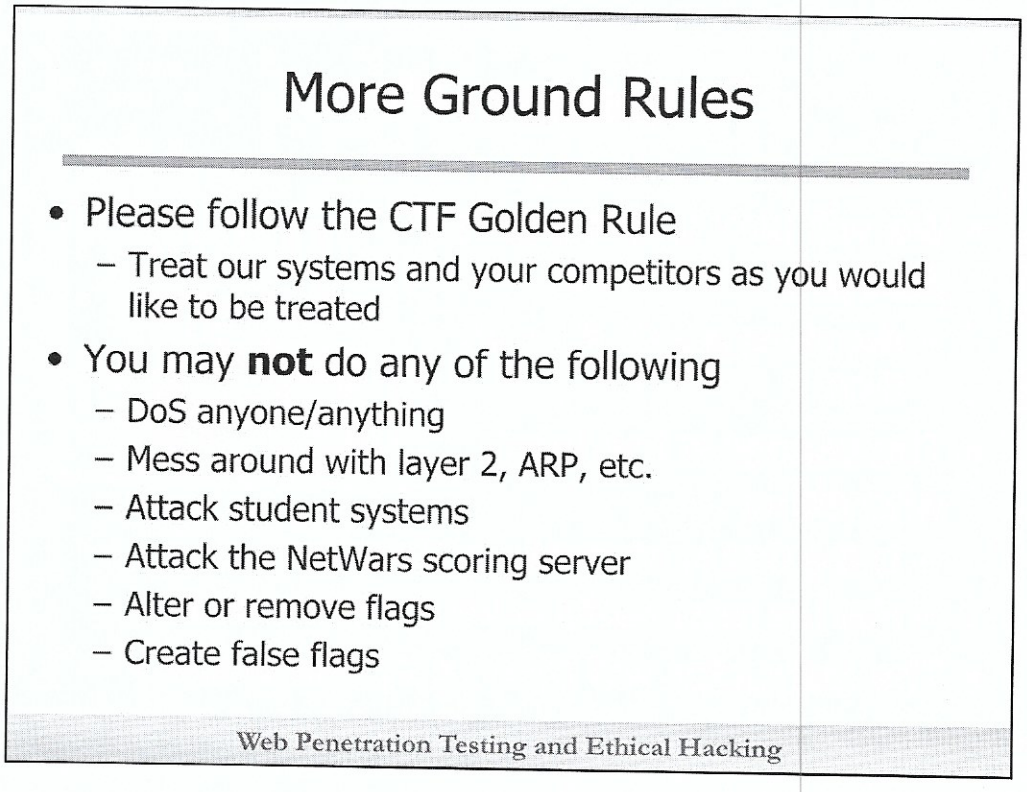
It may go without saying: but **read the questions carefully**! Students often lose points due to carelessness.

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.



Any web application in the network range of 10.42.5.0/24 is within scope of this test.

You may begin with a nmap scan of this network as you begin to enter answers into the scoring server. The scan will come in handy once level two is unlocked.



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 team who either
  - Is the first to score all the points, or
  - Has the most points when the game ends
- The instructor will then recap the game

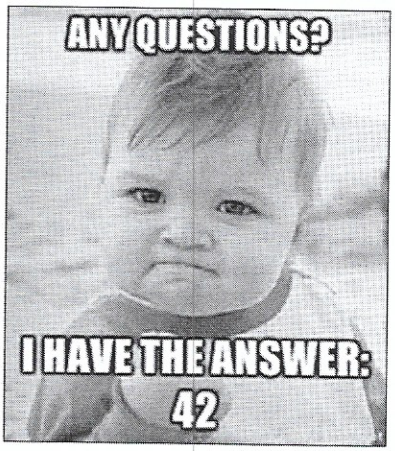
Web Penetration Testing and Ethical Hacking

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: Shodan
- After that, it's up to you!

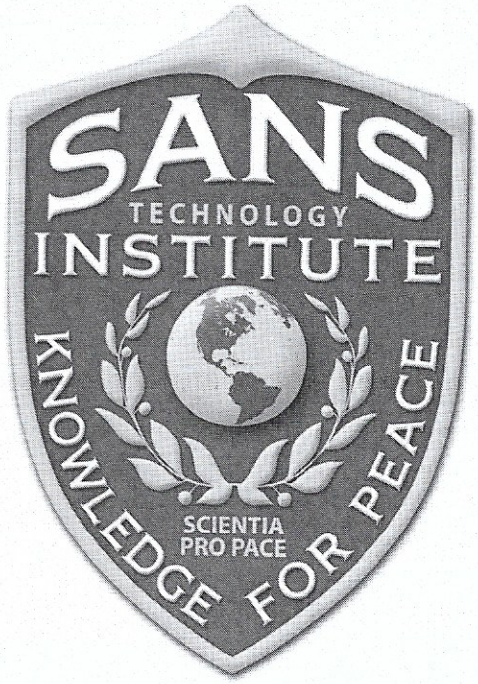


Web Penetration Testing and Ethical Hacking

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



This Course is Part of the SANS Technology Institute (STI) Master's Degree Curriculum.

If your brain is hurting from all you've learned in this class, but you still want more, consider applying for a Master's Degree from STI. We offer two hands-on, intensive Master's Degree programs:

- Master of Science in Information Security Engineering
- Master of Science in Information Security Management

If you have a bachelor's degree and are ready to pursue a graduate degree in information security, please visit www.sans.edu for more information.

www.sans.edu **855-672-6733** **info@sans.edu**

"As usual, SANS courses pay for themselves by Day 2. By Day 3, you are itching to get back to the office to use what you've learned."
Ken Evans, Hewlett Packard Enterprise - Digital Investigation Services

SANS Programs
sans.org/programs

GIAC Certifications
Graduate Degree Programs
NetWars & CyberCity Ranges
Cyber Guardian
Security Awareness Training
CyberTalent Management
Group/Enterprise Purchase Arrangements
DoDD 8140
Community of Interest for NetSec
Cybersecurity Innovation Awards

Search SANSInstitute

SANS Free Resources
sans.org/security-resources

- E-Newsletters
  NewsBites: Bi-weekly digest of top news
  OUCH!: Monthly security awareness newsletter
  @RISK: Weekly summary of threats & mitigations
- Internet Storm Center
- CIS Critical Security Controls
- Blogs
- Security Posters
- Webcasts
- InfoSec Reading Room
- Top 25 Software Errors
- Security Policies
- Intrusion Detection FAQ
- Tip of the Day
- 20 Coolest Careers
- Security Glossary

SANS Institute
8120 Woodmont Avenue | Suite 310
Bethesda, MD 20814
301.654.SANS(7267)
info@sans.org