

542.6

Capture the Flag



SANS

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

542.6

Capture the Flag

SANS

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

Copyright © 2016, The SANS Institute. All rights reserved. The entire contents of this publication are the property of the 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 THE SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, the 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 the SANS Institute to the 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 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.

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 THE SANS INSTITUTE, AND THAT THE 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 the 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 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.

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.

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



Web Penetration Testing and Ethical Hacking Capture the Flag

SANS Security 542.6

Seth Misenar (GSE #28) & Eric Conrad (GSE #13)

Copyright 2016, Kevin Johnson, Eric Conrad, Seth Misenar

All Rights Reserved

Version B02_02

Web Penetration Testing and Ethical Hacking

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!

VM Configuration

- Please follow these instructions to change from host-only mode to bridged mode and receive a DHCP address
1. Connect your laptop to the nearest switch
 2. Set the Security542 VM to Bridged networking
 - In VMware Player, go to Player -> Removable Devices -> Network Adapter -> Settings (see notes 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

Web Penetration Testing and Ethical Hacking

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

Teams

- Work in teams
 - Between two and five people
- Winning teams are multithreaded
 - Always work different angles
 - Do not "monotask"
- Have regular "meetings"
 - Review what you have
 - Compare notes
 - Adjust and plan your next steps

Web Penetration Testing and Ethical Hacking

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.

Connect to the Scoring Server

- Type the following from both to verify connectivity:
 - Linux: \$ **ping 10.42.42.42**
- Then surf to: **https://10.42.42.42**
 - Note the “**s**” in https!
 - You may use whichever browser/OS is most convenient for you
 - Note: cut and paste will be very helpful!

Web Penetration Testing and Ethical Hacking

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

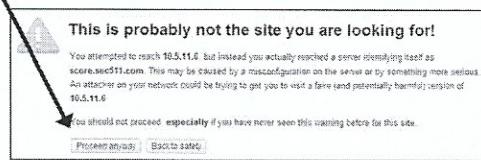
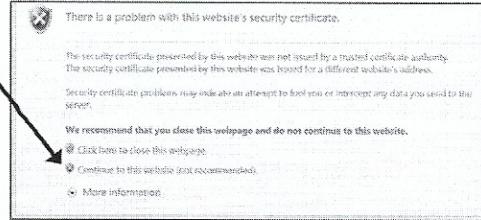
\$ **ping 10.42.42.42**

C:\> **ping 10.42.42.42**

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

Accept the Certificate

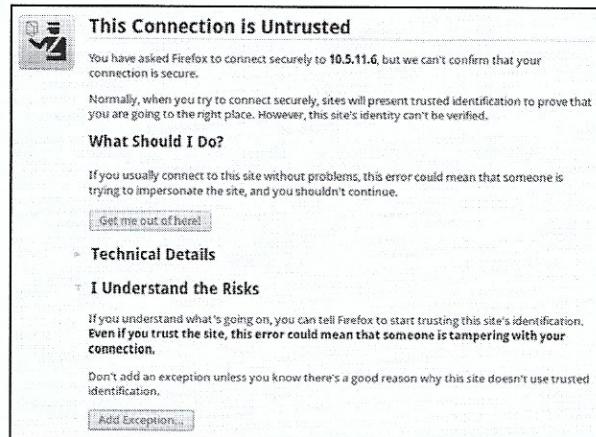
- IE: ***Continue to this website***
- Chrome: ***Proceed anyway***
- Firefox: see notes



Web Penetration Testing and Ethical Hacking

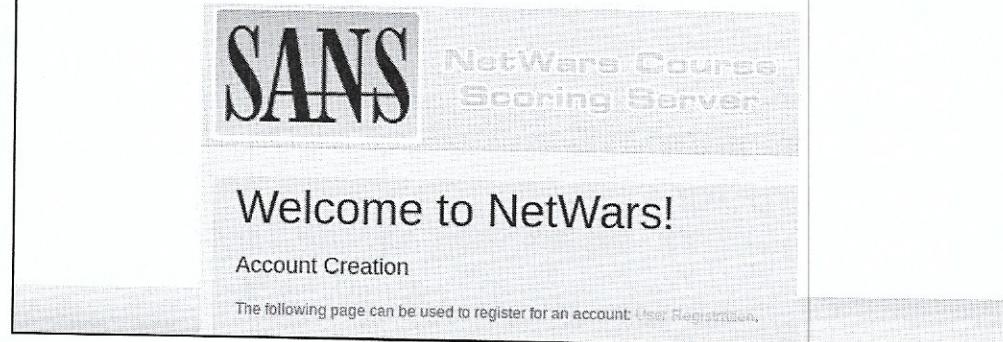
Firefox requires three steps:

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



Create an Account

- Go to <https://10.42.42.42>
 - Then: User Registration
 - You may create a shared team account
 - Simultaneous account logins is supported



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

User Registration

Username: VogenPoetsSociety Mixed case alphanumeric [A-Z_], 4-32 characters

Password: Must be at least 5 characters long

Password Confirmation: Please re-type your password

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)

Name that search engine - (10 pts)

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 question must be answered correctly before proceeding*)

Flag:

Convert to SHA1

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

Hints

- **Some** questions have up to three hints
 - The more difficult questions have hints
 - Easier questions do not
- Hints deduct points **immediately**
- First hint: deduct 30% available points
 - “Go to 542.2 Shellshock section, pay careful attention to the Shellshock exercise”
- Second hint: deduct another 30% available points
 - “Let’s use curl! Just like we did in the Shellshock exercise!”
- Third hint (deducts all available points for that question):
 - Step-by-step instructions for completing the challenge

Web Penetration Testing and Ethical Hacking

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.

Hint Example

- A sample question is worth 10 points
 - You request a hint, which immediately deducts 3 points from your score
 - You then answer the question, winning 10 points, for a net gain of 7 points (10 minus 3)
- Worst-case example (10 point question):
 - Request first (-3 points) and second hint (-3 additional points)
 - If you are still stuck: request the final hint (-4 points), which will provide the answer
 - Then answer the question, for a net gain of 0 points

Web Penetration Testing and Ethical Hacking

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

- Today's goals:
 - Put everything we have learned this week into hands-on practice
 - Learn
 - Have fun while competing to win
- Hints can be used strategically and/or to complete difficult challenges
- **Anyone** may complete most of the CTF

Web Penetration Testing and Ethical Hacking

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...”

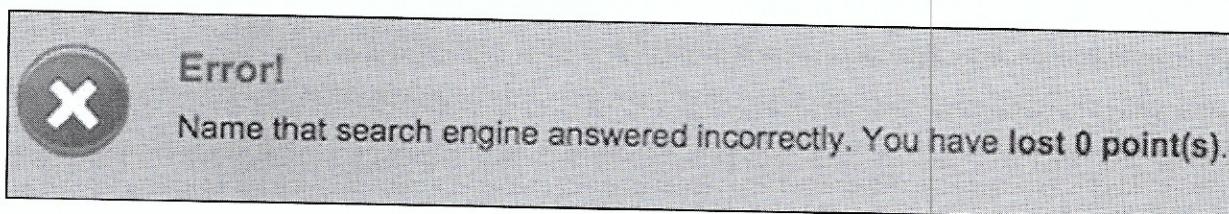
The capstone provides an opportunity to learn, and/or an opportunity to compete. You may choose the “no hints” method to maximize points, the “more hints” method to maximize learning, or a combination of the two methods.

How It Works

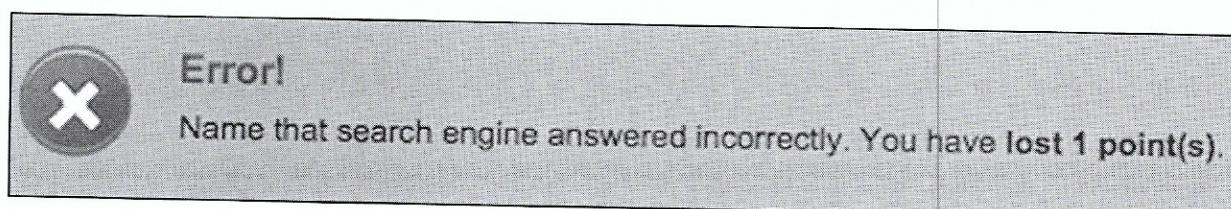
- There is no penalty for one wrong answer to a question
- After that, each wrong answer deducts a point from your total
- This is done to
 - Encourage high quality work
 - Discourage blind guessing, brute forcing, etc.
- **Do not** reload the page immediately after a wrong answer
 - Some browsers will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

Web Penetration Testing and Ethical Hacking

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

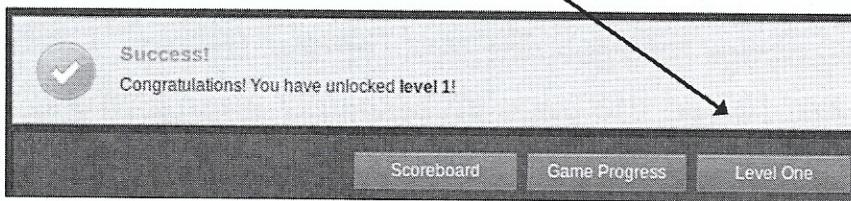
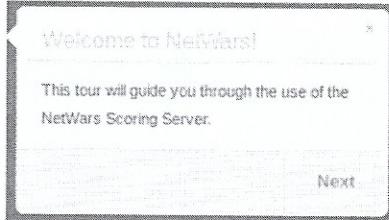


There is a one-point penalty for each incorrect answer after the first:



Once the Instructor Gives the Green Light

- Log into the scoring server
- Take the tour! →
- Then go to "Level One"



Web Penetration Testing and Ethical Hacking

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."

Flags with SHA1 Answers

- “Flag” answers must be hashed (SHA1)
 - These will have a “Convert to SHA1” option

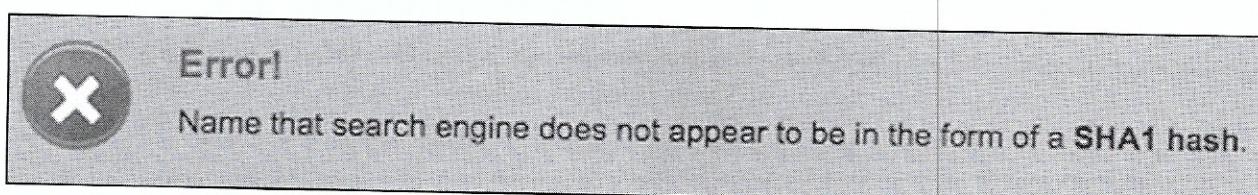
The screenshot shows a web-based penetration testing interface. At the top, it says "Name that exploit - (10 pts)". Below that, it asks to examine an exploit string: "() { :;};echo;/bin/cat /etc/passwd". It then asks what the name of the vulnerability is, specifying that the answer should be a word with only the first letter capitalized. The correct answer is "Shellshock". To the right of the question is a "Convert to SHA1" button. Below the question, the flag is shown as "Flag: 063f2f86cd85ff4ab8664148c61d1ab830c04990". A large arrow points from this flag to the right, labeled "Converted answer". At the bottom of the interface, it says "Web Penetration Testing and Ethical Hacking".

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.



Answering Your First Question

- Answer the first question
 - Enter “Shodan” and press “Convert to SHA1”
 - Then submit the answer

The screenshot shows a challenge interface with the following details:

- Name that search engine - (10 pts)**
- 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 question must be answered correctly before proceeding*)
- Flag: Shodan
- Convert to SHA1
- Success!** Name that search engine answered correctly. You have earned 10 point(s).
- Web Penetration Testing and Ethical Hacking

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!

Game Advice

- Read the questions ***very*** carefully
 - Every word counts!
 - SHA1 is **very** unforgiving of sloppiness!
- Everything you need to win is in the room
 - Contained in your VM or in a local network resource that will be referenced
 - Internet access is not needed to complete any challenge
- If the challenge states that it is based on a specific server or service, then target those
 - Do not add unrelated data to the challenge!

Web Penetration Testing and Ethical Hacking

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.

Project Scope

- Internet and intranet web applications are in scope
- All web applications on the target network of 10.42.5.0/24 are in scope
 - You may scan this range
 - You may also steal credentials to gain interactive access to systems via other protocols (such as ssh)
- There is a DNS server at 10.42.5.24
 - There may be targets without DNS entries
- The NetWars scoring server will offer specific guidance on individual challenges

Web Penetration Testing and Ethical Hacking

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.

More Ground Rules

- Please follow the CTF Golden Rule
 - Treat our systems and your competitors as you would like to be treated
- You may **not** do any of the following
 - DoS anyone/anything
 - Mess around with layer 2, ARP, etc.
 - Attack student systems
 - Attack the NetWars scoring server
 - Alter or remove flags
 - Create false flags

Web Penetration Testing and Ethical Hacking

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



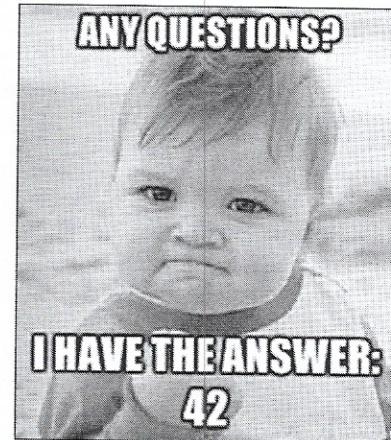
Web Penetration Testing and Ethical Hacking

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!



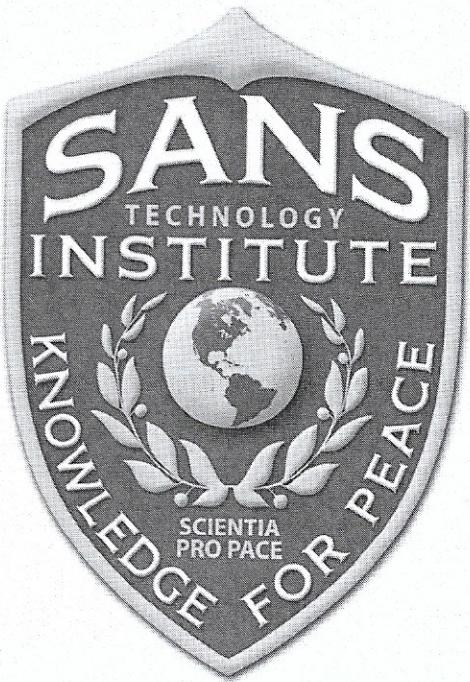
Web Penetration Testing and Ethical Hacking

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