Welcome!

❒ Instructor: Dr. Yoohwan Kim, CISSP, CEH, CPT, CISA
  ○ Associate Professor at Computer Science
  ○ Office: SEB 4245,  Phone: 895 - 5348
  ○ E-mail: Yoohwan.Kim@unlv.edu
  ○ Office hours: Mon & Web, 4:00pm– 6:00pm, or by appointment

❒ Graduate Assistant:
  ○ TBD
  ○ GA office hours: TBD
  ○ GA office location: SEB 4236 Lab

❒ Class web page:
  ○ Visit WebCampus (http://webcampus.unlv.edu)
  ○ Course material, assignments, quiz, scores will be posted
About the Course

❖ Class web page
  ❖ Visit WebCampus
    (https://webcampus.unlv.edu)
  ❖ All course material, assignments will be posted

❖ Textbook
  ❖ CEH v9: Certified Ethical Hacker
    • May 2016, 648 pages
    • ISBN-10: 1119252245
  ❖ $33.77 at Amazon
Prerequisites

- Official Prerequisite
  - CS 370 Operating Systems

- Operating systems
  - Windows, Linux
  - Program installation, applications, commands

- Basic programming skills

- Helpful to know, but not required,
  - Computer networks in general
  - Internet protocol suite
  - Computer hacking skills
Quizzes & Exams

- **Quizzes**
  - Seven announced quizzes
  - The worst one (or missing one) will be dropped

- **Exams**
  - Closed books and notes
  - **Midterm**: Mar. 13, Monday (review on Mar. 8, Wed)
  - Final: May 10, Wednesday, 3:10pm – 5:10pm
  - NO make-up exams!!!
  - NO early exams!!!

- **Optional CEH Exam**
  - May 12, Friday 2:00pm – 6:00pm
Assignments

- No written assignments!
- Only the completion of online labs required

- Research presentation (Only for CS 645)
  - Detailed instruction will be given later
  - One class is reserved for presentations
  - Presentation content will be included in the final exam
Lab Requirements (iLabs)

- All labs are online. No physical lab presence required
  - Provided by EC-Council, the CEH granting organization
  - Total 17 labs
  - The account login information will be given after purchasing the subscription
Evaluation

☒ Evaluation
  ☐ Labs: 30%
  ☐ Quizzes & Lab participation: 10%
  ☐ Midterm: 30%
  ☐ Final: 30%
  ☐ Research project (CS 645): 10%

☒ Grade will be curved
Related Courses

- CS 443 Information Assurance
  - ~20% overlap (Cryptography and Networks)

- CS 448/648 Computer Security
  - ~20% overlap (Cryptography and Networks)

- CS 465/665 Computer Networks I
  - ~5% overlap (Networks)

- CS 789 Advanced Network Security
  - < 10%
## Tentative Schedule

<table>
<thead>
<tr>
<th></th>
<th>Monday</th>
<th>Wednesday</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>16-Jan</strong> MLK Holiday</td>
<td>Introduction</td>
</tr>
<tr>
<td>2</td>
<td><strong>23-Jan</strong> System Fundamentals</td>
<td>Cryptography</td>
</tr>
<tr>
<td>3</td>
<td><strong>30-Jan</strong> Footprinting, Quiz 1</td>
<td>Reconnaissance</td>
</tr>
<tr>
<td>4</td>
<td><strong>6-Feb</strong> Scanning networks</td>
<td>Scanning networks, Quiz 2</td>
</tr>
<tr>
<td>5</td>
<td><strong>13-Feb</strong> Enumeration</td>
<td>System hacking</td>
</tr>
<tr>
<td>6</td>
<td><strong>20-Feb</strong> Presidents' Day Holiday</td>
<td>Malware Threats, Quiz 3</td>
</tr>
<tr>
<td>7</td>
<td><strong>27-Feb</strong> Sniffing</td>
<td>Social engineering</td>
</tr>
<tr>
<td>8</td>
<td><strong>6-Mar</strong> Denial-of service, Quiz 4</td>
<td>Midterm Review</td>
</tr>
<tr>
<td>9</td>
<td><strong>13-Mar</strong> Midterm exam</td>
<td>Sessin hijacking</td>
</tr>
<tr>
<td>10</td>
<td><strong>20-Mar</strong> Hacking Web servers</td>
<td>Hacking web applications</td>
</tr>
<tr>
<td>11</td>
<td><strong>27-Mar</strong> SQL Injection, Quiz 5</td>
<td>Hacking wireless networks</td>
</tr>
<tr>
<td>12</td>
<td><strong>3-Apr</strong> Hacking wireless networks</td>
<td>Hacking mobile platforms, Quiz 6</td>
</tr>
<tr>
<td>13</td>
<td><strong>10-Apr</strong> Spring break</td>
<td>Spring break</td>
</tr>
<tr>
<td>14</td>
<td><strong>17-Apr</strong> Evading IDS</td>
<td>Cloud Computing</td>
</tr>
<tr>
<td>15</td>
<td><strong>24-Apr</strong> Physical Security</td>
<td>CS 645 Presentation, Quiz 7</td>
</tr>
<tr>
<td>16</td>
<td><strong>1-May</strong> Final exam and CEH test review</td>
<td>CEH Mock Exam</td>
</tr>
<tr>
<td>17</td>
<td><strong>8-May</strong> N/A</td>
<td>Final exam</td>
</tr>
</tbody>
</table>
Warning

This class teaches dangerous hacking skills.

Any misconduct with this knowledge and tools may result in prosecution, fines, and/or imprisonment.

Do not use them for illegal purposes, use them only with extreme caution.
Cybersecurity Job Market
Cybersecurity = $$$$ 

- The cost of a data breach is $154 per record lost or stolen
  - Healthcare was most at risk, with an average cost per record lost or stolen as high as $363
  - [http://www.reuters.com/article/us-cybersecurity-ibm-idUSKBN0OC0ZE20150527](http://www.reuters.com/article/us-cybersecurity-ibm-idUSKBN0OC0ZE20150527)

*Figure 13. Trends in four data breach cost components over three years*
Consolidated view (FY 2015 = 350, FY 2014 = 315, FY 2013 = 277)
Measured in US$ (millions)
Data Breach is Increasing

- [Link](https://digitalguardian.com/blog/history-data-breaches)

**Annual number of data breaches and exposed records in the United States from 2005 to 2014 (in millions)**

The statistic presents the development of cyber attacks over time. It presents the recorded number of data breaches and records exposed in the United States between 2005 and 2014. In 2014, the number of data breaches in the United States amounted to 783 with more than 85.61 million records exposed.
“Demand to fill cybersecurity jobs booming”

- http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/

- More than **209,000 cybersecurity jobs** in the U.S. are **unfilled**, and postings are **up 74 percent** over the past five years
  - “The number of jobs in information security is going to grow **tenfold in the next 10 years**”
  - Demand for cybersecurity professionals over the past five years grew **3.5 times faster** than demand for other IT jobs and about **12 times faster** than for all other jobs

- ➡️ **better salaries** for information security professionals compared to other IT jobs. Cybersecurity jobs on average offer a premium of about **$12,000 over** the average for all computer jobs
“One Million Cybersecurity Job Openings In 2016”


- Expected to grow from **$75 billion** in 2015 to **$170 billion** by 2020
  - A report from Cisco puts the global figure at one million cybersecurity job openings.
  - Demand is expected to rise to 6 million globally **by 2019**, with a projected **shortfall of 1.5 million**,

- Cybersecurity workers can command an average salary premium of nearly $6,500 per year, or **9% more** than other IT workers
“Cyber-Security Skills Shortage Leaves Companies Vulnerable”

- [http://www.informationweek.com стратегия и риск-стратегия/7-цибер-безопасность-навыки-на-высокий-деманд-/d/d-id/1326494](http://www.informationweek.com стратегия и риск-стратегия/7-цибер-безопасность-навыки-на-высокий-деманд-/d/d-id/1326494)

- The vast majority of participants (82%) reported a lack of cyber-security skills within their organization.
  - One in three say the shortage makes them prime hacking targets

- About half of survey respondents said they prefer entry-level candidates to have a bachelor's degree, but hands-on experience and professional certifications are typically more useful for developing the skills in greatest demand.
## Quick Facts: Information Security Analysts

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2015 Median Pay</strong></td>
<td>$90,120 per year $43.33 per hour</td>
</tr>
<tr>
<td><strong>Typical Entry-Level Education</strong></td>
<td>Bachelor's degree</td>
</tr>
<tr>
<td><strong>Work Experience in a Related Occupation</strong></td>
<td>Less than 5 years</td>
</tr>
<tr>
<td><strong>On-the-job Training</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Number of Jobs, 2014</strong></td>
<td>82,900</td>
</tr>
<tr>
<td><strong>Job Outlook, 2014-24</strong></td>
<td>18% (Much faster than average)</td>
</tr>
<tr>
<td><strong>Employment Change, 2014-24</strong></td>
<td>14,800</td>
</tr>
</tbody>
</table>

## Quick Facts: Web Developers

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2015 Median Pay</strong></td>
<td>$64,970 per year $31.23 per hour</td>
</tr>
<tr>
<td><strong>Typical Entry-Level Education</strong></td>
<td>Associate's degree</td>
</tr>
<tr>
<td><strong>Work Experience in a Related Occupation</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>On-the-job Training</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Number of Jobs, 2014</strong></td>
<td>148,500</td>
</tr>
<tr>
<td><strong>Job Outlook, 2014-24</strong></td>
<td>27% (Much faster than average)</td>
</tr>
<tr>
<td><strong>Employment Change, 2014-24</strong></td>
<td>39,500</td>
</tr>
</tbody>
</table>

# Robert Half Salary Guide 2017

[https://www.roberthalf.com/workplace-research/salary-guides](https://www.roberthalf.com/workplace-research/salary-guides)

<table>
<thead>
<tr>
<th>Title</th>
<th>2016</th>
<th>2017</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SECURITY (F)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Security Analyst</td>
<td>$113,500 - $160,000</td>
<td>$118,250 - $169,000</td>
<td>5.0%</td>
</tr>
<tr>
<td>Systems Security Administrator</td>
<td>$105,500 - $149,500</td>
<td>$110,500 - $157,500</td>
<td>5.1%</td>
</tr>
<tr>
<td>Network Security Administrator</td>
<td>$103,250 - $147,000</td>
<td>$107,750 - $155,250</td>
<td>5.1%</td>
</tr>
<tr>
<td>Network Security Engineer</td>
<td>$110,250 - $152,750</td>
<td>$115,500 - $162,500</td>
<td>5.7%</td>
</tr>
<tr>
<td>Information Systems Security Manager</td>
<td>$129,750 - $182,000</td>
<td>$136,000 - $191,750</td>
<td>5.1%</td>
</tr>
<tr>
<td><strong>WEB DEVELOPMENT (D)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Senior Web Developer</td>
<td>$111,250 - $154,000</td>
<td>$116,250 - $161,500</td>
<td>4.7%</td>
</tr>
<tr>
<td>Web Developer</td>
<td>$ 78,500 - $129,500</td>
<td>$ 82,750 - $135,500</td>
<td>4.9%</td>
</tr>
<tr>
<td>Front-End Web Developer</td>
<td>$ 79,750 - $111,250</td>
<td>$ 83,250 - $119,500</td>
<td>6.2%</td>
</tr>
<tr>
<td>Web Administrator</td>
<td>$ 68,750 - $106,250</td>
<td>$ 70,750 - $111,500</td>
<td>4.1%</td>
</tr>
<tr>
<td>Web Designer</td>
<td>$ 67,000 - $112,250</td>
<td>$ 70,500 - $118,000</td>
<td>5.2%</td>
</tr>
<tr>
<td>E-Commerce Analyst</td>
<td>$ 88,000 - $129,500</td>
<td>$ 92,000 - $135,000</td>
<td>4.4%</td>
</tr>
</tbody>
</table>
Cybersecurity jobs

❒ Career Coach: There’s plenty of jobs to be had in cybersecurity, but only if you are prepared

❖ How?
   o Get certified (e.g., Certified Information Systems Security Professional)
   o Have experience in the military or law enforcement
   o Get IT security experience through volunteer work and internships; offer to help IT professors at a local college or university to gain experience
   o Be willing to work in fast-paced environments with some unpredictability in job hours.
Cybersecurity Certification

A ticket to cybersecurity jobs!
Top Security Certificates

- **CISSP (Certified Information Systems Security Professional)**
  - A high-level credential focused on security policy and management.
  - The most frequently mentioned certification in the business.
  - Requires 5 year job experience

- **CISM (Certified Information Security Manager)**
  - Geared towards people in managerial positions (e.g. CIO of IT security).
  - Requires 5 year job experience. $450.
  - [http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx](http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx)

- **CISA (Certified Information Systems Auditor)**
  - Designed for professionals who audit, control, monitor and assess information technology and business systems.
  - Requires 5 year job experience. $710

- **OSCP (Offensive Security Certified Professional)**
  - Designed for pen testers and includes a rigorous 24 hour certification exam.
Top Security Certificates

- **GCIH (SANS GIAC Certified Incident Handler)**
  - For incident handlers responsible for detecting, responding to and resolving computer security incidents.
  - [Visit GCIH Certification Page](http://www.giac.org/certification/certified-incident-handler-gcih)

- **GSEC (SANS GIAC Security Essentials)**
  - No job requirements
  - $1249. [Visit GSEC Certification Page](http://www.giac.org/certification/security-essentials-gsec)

- **CompTIA Security+**
  - Entry level. No job requirements
  - $311. [Visit CompTIA Security+ Certification Page](https://certification.comptia.org/certifications/security+)

- **CEH (Certified Ethical Hacker)**
  - An intermediate-level credential. It's a must-have for IT professionals pursuing careers in ethical hacking.
  - Two years of job requirement or formal training (this class!)
  - $700, [Visit CEH Certification Page](https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/)

- **For more**
  - [Visit Tom's IT Pro Security Certifications Article](http://www.tomsitpro.com/articles/information-security-certifications.2-205.html)
Job Board Search Results

- [http://www.tomsitpro.com/articles/information-security-certifications,2-205.html](http://www.tomsitpro.com/articles/information-security-certifications,2-205.html)

<table>
<thead>
<tr>
<th>Certification</th>
<th>SimplyHired</th>
<th>Indeed</th>
<th>LinkedIn Jobs</th>
<th>TechCareers</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEH</td>
<td>1,977</td>
<td>2,184</td>
<td>1,427</td>
<td>257</td>
<td>5,845</td>
</tr>
<tr>
<td>CISM</td>
<td>3,286</td>
<td>3,585</td>
<td>2,337</td>
<td>10,629</td>
<td>19,837</td>
</tr>
<tr>
<td>CISSP</td>
<td>10,526</td>
<td>11,617</td>
<td>7,632</td>
<td>15,212</td>
<td>44,987</td>
</tr>
<tr>
<td>GSEC</td>
<td>1,317</td>
<td>1,477</td>
<td>954</td>
<td>128</td>
<td>3,876</td>
</tr>
<tr>
<td>Security+</td>
<td>3,038</td>
<td>3,396</td>
<td>1,275</td>
<td>1,431</td>
<td>9,140</td>
</tr>
</tbody>
</table>
## 15 Top Paying IT Certifications In 2016

[link](http://www.forbes.com/sites/louiscolumbus/2016/02/21/15-top-paying-it-certifications-in-2016-aws-certified-solutions-architect-leads-at-125k/#2596f0b66702)

### Most Valuable IT Certifications, 2016
(Source: Global Knowledge Study, 15 Top-Paying Certifications for 2016)

<table>
<thead>
<tr>
<th>Certification</th>
<th>Annual Salary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Web Services Certified Solutions Architect – Associate</td>
<td>$125,871</td>
</tr>
<tr>
<td>Certified in Risk and Information Systems Control (CRISC)</td>
<td>$122,954</td>
</tr>
<tr>
<td>Certified Information Security Manager (CISM)</td>
<td>$122,291</td>
</tr>
<tr>
<td>Certified Information Systems Security Professional (CISSP)</td>
<td>$121,923</td>
</tr>
<tr>
<td>Project Management Professional (PMP®)</td>
<td>$116,094</td>
</tr>
<tr>
<td>Certified Information Systems Auditor (CISA)</td>
<td>$113,320</td>
</tr>
<tr>
<td>Cisco Certified Internetwork Expert (CCIE) Routing and Switching</td>
<td>$112,858</td>
</tr>
<tr>
<td>Cisco Certified Network Associate (CCNA) Data Center</td>
<td>$107,045</td>
</tr>
<tr>
<td>Cisco Certified Design Professional (CCDP)</td>
<td>$105,008</td>
</tr>
<tr>
<td>Certified Ethical Hacker (CEH)</td>
<td>$103,297</td>
</tr>
<tr>
<td>Six Sigma Green Belt</td>
<td>$102,594</td>
</tr>
<tr>
<td>Citrix Certified Professional – Virtualization (CCP-V)</td>
<td>$102,138</td>
</tr>
<tr>
<td>Cisco Certified Networking Professional (CCNP) Security</td>
<td>$101,414</td>
</tr>
<tr>
<td>ITIL® v3 Foundation</td>
<td>$99,869</td>
</tr>
<tr>
<td>VMware Certified Professional 5 – Data Center Virtualization (VCP5-DCV)</td>
<td>$99,334</td>
</tr>
</tbody>
</table>
Salary Trend

https://www.indeed.com/salary?q1=Certified+Ethical+Hacker&l1=
DoD Jobs


- How do we know an IT personnel is proficient?
- Provides guidance and procedures for the training, certification, and management of all government employees who conduct Information Assurance functions
- Requires that anyone who has access to IT system, must be certified with one of the external certifications listed.

 Directive 8140

- With wireless, mobile, cloud, 8570 became outdated
- aka the Information Assurance Workforce Improvement Program

 For more

- [http://www.cyberdegrees.org/resources/certifications/](http://www.cyberdegrees.org/resources/certifications/)
## Certifications in 8570

<table>
<thead>
<tr>
<th>IAT Level I</th>
<th>IAT Level II</th>
<th>IAT Level III</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+ Network+</td>
<td>GSEC Security+</td>
<td>CISA GCiH</td>
</tr>
<tr>
<td>SSCP</td>
<td>GSE</td>
<td>GSE</td>
</tr>
<tr>
<td></td>
<td>SCNP</td>
<td>SCNA</td>
</tr>
<tr>
<td></td>
<td>SSCP</td>
<td>CISSP (or Associate)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IAM Level I</th>
<th>IAM Level II</th>
<th>IAM Level III</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAP</td>
<td>CAP</td>
<td>GSLC</td>
</tr>
<tr>
<td>GISF</td>
<td>GSLC</td>
<td>CISM</td>
</tr>
<tr>
<td>GSLC</td>
<td>CISSP (or Associate)</td>
<td>CISSP (or Associate)</td>
</tr>
<tr>
<td>Security+</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IASAE I</th>
<th>IASAE II</th>
<th>IASAE III</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISSP (or Associate)</td>
<td>CISSP (or Associate)</td>
<td>CISSP - ISSEP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CISSP - ISSAP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CND Analyst</th>
<th>CND Infrastructure Support</th>
<th>CND Incident Reporter</th>
<th>CND Auditor</th>
<th>CND-SP Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>GCIA CEH</td>
<td>SSCP CEH</td>
<td>GCiH CSiH CEH</td>
<td>CISA GSNA</td>
<td>CISSP-ISSMP CISM</td>
</tr>
</tbody>
</table>

---

January 18, 2017

CS 445 – Internet Security

Page 28
Why CEH?

- Only multiple choice, no essay
- No job requirements
- DoD 8570
- Best value!
What is CEH?

- A CEH is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.

- The CEH Program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

- The goal of the ethical hacker is to help the organization take preemptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits.
How to get CEH

- Offered by the International Council of E-Commerce Consultants (EC-Council)
  - https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

- Candidates must pass one exam.
  - A comprehensive five-day CEH training course is recommended, with the exam presented at the end of training.
  - Candidates may self-study for the exam but must submit documentation of at least two years of work experience in information security with employer verification. Education may be substituted for experience, but this is approved on a case-by-case basis.

- CEH credential holders are required to obtain 120 continuing education credits for each three-year cycle.
CEH Exam

- 125 multiple-choice questions
  - Passing score: 70%
  - Four hours (< 2 hours mostly)
  - Web-based (result known immediately)
  - Current version: 9

- Practice exam

- Read FAQ at
  - [https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/](https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/)
Cost of CEH Certification

- With CEH training
  - $2995
  - $2875
  - Exam fees are included

- Without official training
  - Eligibility application fee ($100) &
  - Exam voucher ($700 or $650)
Accredited Training Center (ATC)

- UNLV became an EC-Council ATC in Fall 2016
  - Can offer on-site exam
  - Can offer exam at discount price
  - Can offer material at discount prices
  - Can adopt the official courseware (only if all students purchase the official courseware)

- Optional CEH Exam
  - May 12, Friday 2:00pm – 6:00pm
  - Web-based
  - Need to bring own notebook computer
  - Passing score is roughly equivalent to B- grade
Purchase Options

☐ Discount exam voucher
  ○ $300 (Originally $750 - $800)

☐ The official CEH Courseware (Officially required to take the discount exam)
  ○ Besides, our textbook is not adequate for taking the exam
  ○ Print: $325 (eBook: $292.5)

☐ iLabs
  ○ Required for every students in this class
  ○ $125 (originally $200)

☐ Bundle of all 3 above
  ○ Print: $724 (eBook: $691.50)
College Support

- Sands Corporation and a donor pledged some financial support for Cybersecurity certification
  - I will try to have college reimburse $200 for the exam voucher
  - (may be reduced depending on the number)

- Bundle of all 3 above, after reimbursement
  - Print: **$524** (eBook: $491.50)

- Sign up for the intention list
  - If you cannot decide now, send me an email by tomorrow (Thursday) 9:00pm.
  - Will arrange ordering process accordingly
Questions?
Chapter 1. Introduction to Ethical hacking
Computer Security goals - CIA Triad

Confidentiality

Data and services

Integrity

Availability
CIA Triad

☀ Confidentiality
  ○ Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
  ○ A loss of confidentiality is the unauthorized disclosure of information.

☀ Integrity
  ○ Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
  ○ A loss of integrity is the unauthorized modification or destruction of information.

☀ Availability
  ○ Ensuring timely and reliable access to and use of information.
  ○ A loss of availability is the disruption of access to or use of information or an information system.
Security terminology

- **Authentication**
  - assurance that communicating entity is the one claimed
  - have both peer-entity & data origin authentication

- **Access Control**
  - prevention of the unauthorized use of a resource

- **Non-Repudiation**
  - protection against denial by one of the parties in a communication
Security terminology

- **Threat**
  - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
  - That is, a threat is a possible danger that might exploit a vulnerability.
  - Network Threats (sniffing, DoS), Host Threats (malware, privilege escalation), Application Threats (SQL injection)

- **Threat Modeling**
  - An approach for analyzing the security of and application
Security Terminology

- **Attack**
  - An intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.
  - OS attack (buffer overflow..), misconfiguration attack, application level attack (session hijacking..), shrink-wrap code attack (use of vulnerable common library)

- **Vulnerability**
  - Weakness in the security system that might be exploited

- **Control**
  - An action, device, procedure or technique that removes or reduces a vulnerability

- **Defense in Depth**
  - Multiple protection layers
A Threat is blocked by Control of a Vulnerability
Overview of Hacking
Hacking in movie
Hacking

- What is hacking (originally)?
  - Modifying, improving software or system quickly with kludge
  - Not necessarily a bad term, but more often used for negative aspect

- Now
  - Exploiting system vulnerabilities and compromising security control to gain unauthorized or inappropriate access to system resource
  - Includes not only gaining access, but all activities for collecting information, using service illegally, or modifying/damaging targets
  - More accurate term is cracking or network attack or computer crime
Hackers

- **Types of hackers**
  1. **White hat**: Upon discovering a vulnerability in a computer system, alerts the system vendor to the problem.
  2. **Gray hat**: Supplies information about a security issue both to the vendor and to crackers.
  3. **Black hat**: Exploit system security breaches for nefarious ends.

- **Other types**
  - Suicide hackers (brings down critical infrastructure)
  - Script kiddies
  - Cyber terrorists
  - State-sponsored hackers
  - Hacktivists

- Hackers are not necessarily geniuses. Just have right tools + know how to use them + a lot of sweat.
Defcon – Capture The Flag

- Hackers’ events
  - Defcon
    - Every July (or August) in Las Vegas, www.defcon.org
  - Black Hat
    - In Las Vegas just before Defcon, http://www.blackhat.com/
Hacking Phases

1. Reconnaissance
2. Scanning
3. Exploit (Gaining Access)
4. Keeping access
5. Clearing tracks
1. Reconnaissance

- Reconnaissance
  - Collect information about target (addresses, names, emails, employees, clients, machine names)
  - Not very technical

- How
  - Domain registration
  - DNS zone transfer
  - Web site search
    - PR, white paper, key people, contacts, job ads
  - Google
2. Scanning - Survey the target

- Footprinting and Enumeration
  1. Network mapping
     - blueprint
  2. Port scanning
     - find an entry
  3. OS fingerprinting
     - What OS does the victim run?
  4. Vulnerability scanning
     - How can we penetrate?
  5. Web server / CGI scanning
     - Is the web server vulnerable?
3. Gaining Access

- The culmination of hacking!
  - When written in a script, it may take only a few seconds

- Many ways
  1. Passive sniffing (web pages, pictures, username/passwords...)
  2. Active sniffing (capture & replay, modify/craft packets & inject)
  3. Session hijacking
  4. DNS cache poisoning
  5. IP address spoofing (impersonation)
  6. Buffer overflow
  7. Privilege escalation
  8. Auto pilot (Metasploit)

And much more!
4. Keeping the Access

- Hackers hide customized programs in victims’ machine
  - Rootkit
- Trojan horse
  - Replace users program
- Backdoors
  - Accessing later
  - Keystroke logger, remote control…
- Use it to launch further attacks
5. Clearing Tracks

- Covering the track
  - Delete or modify log files
  - Clean up downloaded/compiled files

- Make forensic analysis difficult
Ethical Hacking

- Identifying vulnerabilities using the hacking tools and techniques
- Performed with the permission of the concerned authorities
- Need both technical and non-technical skills work ethics, policies, standards, laws)

- Ethical Hacker = Penetration tester = White hat hacker
Why do an ethical hack?

Most IT departments are concerned with building system, not breaking
- Important to take attackers point of view

Ethical hacking answers
- What can the attackers see?
- What can they do with it?
- Are all components adequately protected?
- Comply with Industry and legal standards?
Blue Teaming / Red Teaming

- Blue = defenders
- Red = attackers

- Red team test categories
  - Black box testing (zero knowledge)
  - White box testing (complete knowledge)
  - Grey box testing (Partial knowledge)
Next class

- Chapter 2. System Fundamentals
  - Operating systems
  - Networks