Course Mechanics

- Course URL: [http://cs.gmu.edu/~astavrou/isa564_F15.html](http://cs.gmu.edu/~astavrou/isa564_F15.html)

- Instructor – Angelos Stavrou
  - Email: astavrou@gmu.edu
  - Office: Research I, Rm 437
  - Office Phone: (703) 993-1659 & 3772
  - Office Hours: Wednesday 4:30pm – 6:30pm, and by appointment
Course Mechanics

- Course URL:
  - [http://cs.gmu.edu/~astavrou/isa564_F15.html](http://cs.gmu.edu/~astavrou/isa564_F15.html)

- TA – Maofei Chen
  - Email: mchen18(_)gmu.edu
  - Office: ENGR 5321
  - Office Hours: Tuesday: 2:30pm - 4:30pm & Wednesday: 3:00pm - 5:00pm
Course Overview

- Provide hands-on experience with commodity software and their vulnerabilities in a live laboratory environment.
- Experiment with Attacks against Networks and Machines
- Defenses, Forensics and diagnostics for security
- Install and Test Defenses including Intrusion and anomaly detection Systems (IDS)
  Examine the functionality of Botnets, Malware, anti-virus, anti-spyware
Prerequisites

- **Courses**
  - C or better in CS 310 Data Structures and CS 367 Computer Systems & Programming or Equivalent

- **Skills**
  - Familiar or comfortable with Linux
  - C and ASM knowledge is a plus
  - Willingness to spend time in the lab learning about exploits, defenses, and tools.
  - Being able to install programs and work in unix and windows environment
Course Topics (tentative)

- **Introduction**
  - Lab Environment
  - Wireshark & Metasploit
  - Setup your environment

- **Software Vulnerabilities**

- **Crafting Malware**

- **Remote Exploits & Elevation**

- **Defenses: Firewalls/IDSes**

- **Wireless Attacks**

- **Other “Hot” Topics**
  - Emerging infection vectors
  - Advanced malware (e.g., rootkits, botnets)

Labs

- Lab 1: Buffer Overflows
- Lab 2: Network Reconn.
- Lab 3: Malware & Shellcode
- Lab 4: Network Attacks & Remote Exploitation
- Lab 5: Firewalls & Intrusion Detection
- Lab 6: Wireless Exploitation
- Lab 7: Web Vulnerabilities
Course Topics (tentative)

- Introduction
  - Lab Environment, be able to run experiments at home
- Software Vulnerabilities
  - What are the popular attack targets?
- Malware Design & Economics
  - How, What, Why?
- Network Attacks (Wireless)
  - Effectiveness, ease of deployment, traceability
Course Topics (tentative)

- **Defenses I: Intrusion and Firewalls**
  - Capabilities, Ease of use, Limitations

- **Defenses II: Traffic Analysis & Adaptive Firewalls**
  - Can we characterize traffic inside an organization?

- **Defenses III: Host-based Defenses**
  - Host-based Containment architectures
  - Full Virtualization vs para-virtualization vs Lightweight Process Containers

- **Other “Hot” Topics**
  - Emerging infection vectors
  - Virtualization (OpenVZ, Linux Vservers)
  - Advanced malware (e.g., rootkits, botnets)
# Course Grading

<table>
<thead>
<tr>
<th>Topics</th>
<th>Duration (Weeks)</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class participation</td>
<td></td>
<td>5%</td>
</tr>
<tr>
<td>Lab 1: Buffer Overflows</td>
<td>2</td>
<td>10%</td>
</tr>
<tr>
<td>Lab 2: Network Penetration</td>
<td>1</td>
<td>5%</td>
</tr>
<tr>
<td>Lab 3: Malware &amp; Shellcode</td>
<td>2</td>
<td>10%</td>
</tr>
<tr>
<td>Lab 4: Remote Exploitation &amp; Traffic Analysis</td>
<td>2</td>
<td>10%</td>
</tr>
<tr>
<td>Lab 5: Firewalls &amp; Intrusion Detection Systems</td>
<td>2</td>
<td>10%</td>
</tr>
<tr>
<td>Lab 6: Wireless Exploitation</td>
<td>2</td>
<td>10%</td>
</tr>
<tr>
<td>Lab 7: Web Vulnerabilities</td>
<td>1</td>
<td>5%</td>
</tr>
<tr>
<td>Midterm</td>
<td>1</td>
<td>15%</td>
</tr>
<tr>
<td>Final or Team Project</td>
<td>4</td>
<td>20%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>100%</td>
</tr>
</tbody>
</table>
Course Policies

- **Academic integrity**
  - [Read the GMU honor code](#)
  - I want you to collaborate and ask questions, however…

- Unless otherwise noted, work turned in should reflect your independent capabilities
  - If unsure, note / cite sources and help

- Usually, no late submissions will be accepted
  - You will be given two weeks to submit your work
  - No penalty for documented emergency (e.g., medical) or by prior arrangement in special circumstances
Warning

- Policy on security experiments:
  - you may **not** break into machines that are not your own
  - you may **not** attempt to attack or subvert system security on machines not owned by you
  - you can collaborate but **not copy or outsource** your work
Introduction
Lab Environment

- VMware-based VM images
  - VM1: Linux Fedora Core 5
  - VM2: Windows 2000/Linux Fedora Core 5
    - Or Linux Fedora Core 5

- Make sure VMware is installed
  - You may choose to install VMware Server in your own machine
Intro - Wireshark & Metasploit

1: Target Probing

2: Vulnerability Exploitation

Fixed Target

3: Payload

Remote Shell Creation

Attacker

Victim

Windows/Linux

Server or Desktop

or Mobile
Intro - Wireshark & Metasploit

1: Target Probing
2: Vulnerability Exploitation
3: Payload

Wireshark

Attacker

Windows/Linux

Victim

Server or Desktop or Mobile
Lab 1 - Shellcode

1: Target Probing

2: Vulnerability Exploitation

3: Payload

Attacker

Windows/Linux

Victim

Server or Desktop or Mobile
Lab 1 – Buffer Overflow

1: Target Analysis

2: Vulnerability Exploitation

An Example Buffer Overflow

Software Target

3: Exploit

Attacker

Victim

Windows/Linux

Server or Desktop or Mobile
Lab2 – Network Reconnaissance & Penetration

1: Target Probing

2: Vulnerability Identifications

3: Open Ports

Fixed Target

Attacker

Windows/Linux

Victim

Server or Desktop or Mobile
Lab 2 – Network Reconnaissance & Penetration

Attacker

Windows/Linux

Fixed Target

1: Target Probing

2: Vulnerability Identifications

Victim

Server or Desktop or Mobile

3: Open Ports
Lab 3 – Malware & Shellcode

1: Target Probing
2: Vulnerability Exploitation
3: Infect & Download Malware

Attacker

Victim

Windows/Linux

Server or Desktop
or Mobile
Lab 4 – Network Attacks & Exploitation

1: Target Probing
2: Vulnerability Exploitation
3: Target Service

Identify Target

Deny Service, Manipulate Service

Linux

Attacker

Victim

Denial of Service & Session Hijacking

Linux
Lab 5 – Firewalls and IDSes
Lab 5 – Firewalls and IDSes

1: Target Probing
2: Vulnerability Exploitation
3: Payload

Attacker

Windows/Linux

Snort

Victim

Server or Desktop or Mobile
Lab 6 – Wireless Exploitation

1: Wireless Target Probing
2: Protocol Vulnerability Exploitation
3: Spoof Traffic

Attacker

Sniff/Attack

Victim

Windows/Linux

Server or Desktop or Mobile
Lab 7 – Web Vulnerabilities

Attacker

Fedora Core 5
Linux

Fixed Target

1: Target Probing

2: Vulnerability Exploitation

XSS/SQL Injection

Victim

Cookie Stealing, and Others ...

3: Payload

Windows 2000
Lab Environment

- Make sure VMware is installed
  - You may choose to install VMware Workstation in your own machine
    - License: [http://labs.vse.gmu.edu/index.php/FAQ/VMWare#ab](http://labs.vse.gmu.edu/index.php/FAQ/VMWare#ab)

- Work with VMware
  - Example VM Images
    - Kali Linux: [https://www.kali.org/downloads/](https://www.kali.org/downloads/)

- Next Lecture
  - Introduction to Buffer Overflows
    - Be prepared!