ISA 564
SECURITY LAB

Introduction & Class Mechanics
Course Mechanics

- **Course URL:**
  - [http://cs.gmu.edu/~astavrou/isa564_F16.html](http://cs.gmu.edu/~astavrou/isa564_F16.html)

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

- Course URL:

- TA – Maofei Chen
  - Email: mchen18(_)gmu.edu
  - Office: ENGR 4456
  - Office Hours: Monday: 3:30 - 5:00pm & Wednesday: 2:50 - 4:20pm
Course Mechanics

- **Course Content:**
  - Forms on Blackboard
  - Assignments:
    - git.gmu.edu/isa564F16/

- **Instructor – Angelos Stavrou**
  - astavrou@gmu.edu
  - http://www.cs.gmu.edu/~astavrou/isa564_F16_syllabus.html
  - http://www.cs.gmu.edu/~astavrou
Course Overview

- Real world vulnerabilities, exploits, and defense
- First hand experience with security experiments
  - Network/host attacks, defenses, forensics, diag
  - Install and test defenses including Intrusion and anomaly Detection Systems (IDS)
  - Examine the functionality of Botnets, Malware, anti-virus, anti-spyware
- Obtain a deep enough understanding of existing tools (and the security concepts they implement) to not be a script kiddie
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
Skills Survey

- Take a minute to fill out skills survey
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: Malware & Shellcode
Lab 3: Network Attacks & Remote Exploitation
Lab 4: Firewalls & Intrusion Detection
Lab 5: Wireless Exploitation
Lab 6: 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>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class participation</td>
<td>10%</td>
</tr>
<tr>
<td>Labs 5 - 6</td>
<td>50%</td>
</tr>
<tr>
<td>Midterm</td>
<td>15%</td>
</tr>
<tr>
<td>Final or Team Project</td>
<td>25%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></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
Lab Environment

- VMWare-based VM images
  - VM1: Kali Linux
  - VM2: Metasploitable

- 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
3: Payload

Fixed Target

Remote Shell Creation

Attacker

Victim

Windows/Linux

Server or Desktop or Mobile

Browser/Flash/others
Intro - Wireshark & Metasploit

- Attacker
- Victim

1: Target Probing
2: Vulnerability Exploitation
3: Payload

Wireshark

Attacker

Windows/Linux

Server or Desktop or Mobile

Intro - Wireshark & Metasploit

1: Target Probing
2: Vulnerability Exploitation
3: Payload

Wireshark

Attacker

Windows/Linux

Server or Desktop or Mobile
Lab 1 - Shellcode

1: Target Probing
2: Vulnerability Exploitation
3: Payload

Attacker

Victim

Windows/Linux

Server or Desktop or Mobile
Lab 1 – Buffer Overflow

1: Target Analysis

2: Vulnerability Exploitation

Software Target

3: Exploit

An Example Buffer Overflow

Attacker

Victim

Windows/Linux

Server or Desktop or Mobile
Lab 2 – Malware & Shellcode

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

Attacker

Victim

Windows/Linux

Server or Desktop
or Mobile
Lab 3 – Network Attacks & Exploitation

1: Target Probing

2: Vulnerability Exploitation

3: Target Service

Deny Service, Manipulate Service

Identify Target

Denial of Service & Session Hijacking

Attacker

Victim

Linux

Linux
Lab 4 – Firewalls and IDSes

1: Target Probing
2: Vulnerability Exploitation
3: Payload

Attacker

Victim

Windows/Linux

Server or Desktop or Mobile

Snort
Lab 5 – Wireless Exploitation

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

Attacker

Windows/Linux

Victim

Server or Desktop or Mobile
Lab 6 – Web Vulnerabilities

1: Target Probing

2: Vulnerability Exploitation

3: Payload

Attacker

Fedora Core 5

Linux

Victim

Cookie Stealing, and Others...

Windows 2000
Lab Environment

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

- GMU Internal Gitlab instance
  - Login at git.gmu.edu,
    - If does not show in your projects, then contact me
    - Upload public key: Profile, SSH Key, Add SSH Key, copy contents of ~/.ssh/id_rsa.pub
  - For Windows, install clients from git-scm.com/download
  - git clone [git@git.gmu.edu:astavrou/isa564F16.git](git@git.gmu.edu:astavrou/isa564F16.git)

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

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