Syllabus: AIT 671 - Information Systems Infrastructure Lifecycle Management

Term: Fall 2018

Instructor: Jay Holcomb, Adjunct Faculty, Department of Information Sciences and Technology, Volgenau School of Engineering

GMU Website: https://mason.gmu.edu/~jholcom9/
E-mail: jholcom9@gmu.edu

Course: AIT 671 -- Information System Infrastructure Lifecycle Management

Examines information system infrastructure lifecycle management including the audit process, IT governance and best practices, system and infrastructure control, IT service delivery and support, protection of information assets, physical security, business and disaster recovery.

Credits: 3

Day/Time: Thursday, 4:30pm – 7:10pm

Where: Planetary Hall Room: 126

Textbooks (Required):


Other Resources:
Paper readings and Internet resources posted on Blackboard -- AIT 671 Course
Course Goals:
1. Obtain in-depth knowledge on various security systems examples.
2. Gain increased understanding of attack models used against security systems.
3. Learn how security systems provide defenses and counter measures against attack vectors.
4. Understand overall evaluation and management of security systems life cycle.

Course Expectations:
1. Graduate education requires dedication and organization. Proper preparation is expected every week. You are expected to log into our Blackboard course each week and complete any assignments and activities on or before due dates.
2. Students must check their GMU email messages on a daily basis for course announcements, which may include reminders, revisions, and updates.
3. It is expected that you will familiarize yourself with and adhere to the Honor Code. (https://oai.gmu.edu/the-mason-honor-code-2/) Student members of the George Mason University community pledge not to cheat, plagiarize, steal, and/or lie in matters related to academic work.
4. It is essential to communicate any questions or problems to me promptly.

Learning Community:

This course is supported via Blackboard Courses (Log into https://mymason.gmu.edu/ select the Courses Tab, and the course can be found in the Course List).

Each week begins on Monday and ends on Sunday.

In our online learning community, we must be respectful of one another. Please be aware that innocent remarks can be easily misconstrued. Sarcasm and humor can be easily taken out of context. When communicating, please be positive and diplomatic!
Grading policy:

Grades will be determined based on the following:

<table>
<thead>
<tr>
<th>Grade Component</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Cyber Event Paper #1</td>
<td>10%</td>
</tr>
<tr>
<td>Current Cyber Event Paper #2</td>
<td>10%</td>
</tr>
<tr>
<td>In-class Labs or Alternate Assignments (5 @ 5%)</td>
<td>25%</td>
</tr>
<tr>
<td>Team Paper – User Training Pro / Cons</td>
<td>15%</td>
</tr>
<tr>
<td>Team Project and Presentation</td>
<td>30%</td>
</tr>
<tr>
<td>Class Participation</td>
<td>10%</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

The grading scale for this course is:

<table>
<thead>
<tr>
<th>Numeric Grade</th>
<th>Letter Grade</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>97 – above</td>
<td>A+</td>
<td>Passing</td>
</tr>
<tr>
<td>93 – 96%</td>
<td>A</td>
<td>Passing</td>
</tr>
<tr>
<td>90 – 92%</td>
<td>A-</td>
<td>Passing</td>
</tr>
<tr>
<td>87 – 89%</td>
<td>B+</td>
<td>Passing</td>
</tr>
<tr>
<td>83 – 86%</td>
<td>B</td>
<td>Passing</td>
</tr>
<tr>
<td>77 – 82%</td>
<td>B-</td>
<td>Passing</td>
</tr>
<tr>
<td>70 – 76%</td>
<td>C</td>
<td>Passing</td>
</tr>
<tr>
<td>0 – 69%</td>
<td>F</td>
<td>Failing</td>
</tr>
</tbody>
</table>
Current Cyber Event Papers (2 – 10% each = 20%):
Select a recent cyber event - research the event using open source references - write an executive-level technical brief on the event. Include the following at a minimum: threat vector used, vulnerability attacked, business impact of this event, your recommended security system(s) to help provide increased defenses against similar attacks in the future, and why/justification. The length of this paper should be one page - maximum of two pages. (One page is a single side of paper) On a separate page include your open source references - minimum of two (2) unique sources are required.

In-class Labs/Alternate Assignments (5 @ 5% = 25%):
Five (5) labs supporting course objectives, recent cyber attacks, and defensive options that may be available to decrease risk to enterprise security systems.

If unable to complete an in-class lab – a written Internet researched paper assignment may be completed. (Must be completed within 2 weeks of the missed lab for credit.)

Team Paper -- User Awareness/Training Debate (15%):
Review, research, and document your team’s position on the value of cost vs. benefit incurred regarding User Security Awareness Training within a corporation.

Team Project and Presentation (30%):
Either a Red team (Penetration testing team) or Security audit consultants -- your team will decide. You will be auditing security systems/security controls currently in place and recommending improvements.

Select a fictitious critical infrastructure company and create a senior executive (CISO/CIO) level report, with accompanying executive briefing, highlighting the "results" of your red team test or security audit.

At a minimum cover what may happen to the company if they do not implement your top four (4) recommendations and are hit with malicious software, or a breach, describing the potential security risk in great detail. Include how your team approached/engaged with the company, standard processes you used, tools (software/hardware), social, and/or physical security testing that you used, time period of the testing, potential business impacts of any major issues you identified, cost of the assessment, team skills with estimated costs, and the [critical] red team/audit report.

The length of the report should be less than 45 pages. (One page is a single side of paper / double-spaced) On a separate attachment include your open source references. (APA formatting applies)

The report and presentation will be given during our final session.

Class Participation (10%):
Active participation in weekly lectures, labs, and team assignments
Course Schedule (Tentative):

Week 1: Introduction to Information Systems Infrastructure Life Cycle Management, Security Planning, and Incident Response

Objective: Develop an understanding of the information systems infrastructure life cycle management process, identify standard security planning requirements for enterprise-wide cybersecurity. In addition, explain the importance of establishing an incident response process in advance of an incident.

Course Goal Connection:
2. Gain increased understanding of attack models used against security systems.
3. Learn how security systems provide defenses and counter measures against attack vectors.
4. Understand overall evaluation and management of security systems life cycle.

Required Reading:
- Read IAD’s Top 10 Information Assurance Mitigation Strategies (December 2015) Posted on Blackboard -- AIT 671 Week 1
- Review: ISC² Cybersecurity Trends 2017 Survey Report
- Review: ISC² IT Professionals are a Critically Underutilized Resource for Cybersecurity

Other Reading (Recommended):
- Paper readings and Internet resources posted on Blackboard -- AIT 671

Week 2: Networking Basics for Cybersecurity Managers

Objective: Identify and describe the basic functions of network assets such as switches, routers, firewalls, servers, workstations and hosts. Discuss and describe the Open Systems Interconnections (OSI) reference model. Compare and contrast the basic functions of network protocols, associated with TCP/IP.

Course Goal Connection:
1. Obtain in-depth knowledge on various security systems examples.
2. Gain increased understanding of attack models used against security systems.
3. Learn how security systems provide defenses and counter measures against attack vectors.
4. Understand overall evaluation and management of security systems life cycle.

Required Reading:
- Review NIST Special Publication 800-100 (March 2007) Chapters 3, 8, and 13
- Read: Cisco -- Internetworking Basics http://www.cisco.com/cpress/ cc/td/cpress/fund/ith/ith01gb.htm
- Read: DHS/US-CERT Alert (TA16-250A) The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations https://www.us-cert.gov/ncas/alerts/TA16-250A
• **Read:** ASD Essential Eight Explained – March 2018
  Posted on *Blackboard* -- AIT 671 Week 2
• **Read:** Verizon - 2016 Data Breach Investigations Report (DBIR)
  Posted on *Blackboard* -- AIT 671 Week 2
• **Read:** Verizon — 2016 Data Breach Digest
  Posted on *Blackboard* -- AIT 671 Week 2
• **Read:** Verizon - 2017 Data Breach Investigations Report (DBIR)
  Posted on *Blackboard* -- AIT 671 Week 2
• **Read:** Verizon - 2018 Data Breach Investigations Report (DBIR)
  Posted on *Blackboard* -- AIT 671 Week 2
• **Read:** The Register — Hackers tear shreds off Verizon’s data breach report top 10 bug list
  Posted on *Blackboard* -- AIT 671 Week 2

**Other Reading (Recommended):**
• Paper readings and Internet resources posted on *Blackboard* -- AIT 671

**Week 2 Assignment:**
• **Hands-on Activity #1 (Not graded)** — in-class activity using cyber tools and processes we have been discussing.

**Week 3: Cybersecurity Fundamentals and “Best Practices” Leaders Should Know**

**Objective:** Identify four (4) best practices every corporate network/user should employ to reduce risk of exploitation of potential cyber vulnerabilities. Explain the benefit of adopting the Critical Security Controls for an organization. Describe three of the 10 OWASP Top 10 Application Security Risks – 2017.

**Course Goal Connection:**
1. Obtain in-depth knowledge on various security systems examples.
2. Gain increased understanding of attack models used against security systems.
3. Learn how security systems provide defenses and counter measures against attack vectors.
4. Understand overall evaluation and management of security systems life cycle.

**Required Reading:**
• **Read:** OWASP -- *Top Ten Project* - 2017
• **Read:** ASD Strategies to Mitigate Cyber Security Incidents (February 2017)
• **Review:** Center for Internet Security, The Critical Security Controls for Effective Cyber Defense Version 7
  http://www.cisecurity.org/critical-controls/
• **Review:** LightCyber -- 2016 Cyber Weapons Report
• **Review:** UK Government, Cyber Essentials Scheme: Requirements for basic technical protection from cyberattacks
• **Review:** Common Vulnerabilities and Exposures (CVE). -- https://cve.mitre.org
• **Review:** National Vulnerability Database (NVD) -- https://nvd.nist.gov
• **Review:** ISACA, Control Objectives for Information and Related Technology (COBIT) 5 open source information -- http://www.isaca.org/COBIT/Pages/default.aspx
• **Preview:** ISO/IEC 27001 - Information security management
Other Reading (Recommended):
- Paper readings and Internet resources posted on Blackboard -- AIT 671

Week 3 Assignment:
- **Current Cyber Event Paper #1**

Week 4: Know Your Network (Sniffing, Scans, Config Management, Patching, etc.)

Objective: Discuss packets and describe packet creation, and explain the Open Systems Interconnections (OSI) reference model. Identify and describe the benefits of configuration management with regards to securing your enterprise. Discuss why patching IT systems/equipment is so critical in reducing your organization’s cybersecurity risk.

Course Goal Connection:
1. Obtain in-depth knowledge on various security systems examples.
2. Gain increased understanding of attack models used against security systems.
3. Learn how security systems provide defenses and counter measures against attack vectors.
4. Understand overall evaluation and management of security systems life cycle.

Required Reading:
- **Review** NIST Special Publication 800-100 (March 2007) -- Chapter 14
- **Review** NIST Special Publication 800-40 (July 2013)
  http://dx.doi.org/10.6028/NIST.SP.800-40r3
- **Review**: NIST Special Publication 800-53 Revision 4 (April 2013)
  Chapters 1 and 2 – with additional concentration on CM family
- **Read**: RTFM: Red Team Field Manual, CreateSpace Independent Publishing Platform; 1.0 edition (February 11, 2014), see lab materials
- **Read**: Oracle, The Importance of Patches
  http://www.oracle.com/technetwork/articles/grid/o10field-088569.html
- **Review**: Wireshark User’s Guide
  https://www.wireshark.org/download/docs/user-guide-us.pdf
  http://sectools.org/tag/sniffers/
- **Watch**: Hak5 YouTube, Wireshark 101: The OSI Model, Hak5 116
  https://www.youtube.com/watch?v=dN8PcdOdcHs&list=PLA2578BDE9CB9AAB3&index=24

Other Reading (Recommended):
- Paper readings and Internet resources posted on Blackboard -- AIT 671

Week 4 Assignment:
- **Lab #1 – in-class lab supporting cyber tools, attack vectors, network defense options and processes we have been discussing**
Week 5: Network Security Systems Overview for Managers (Firewall, IDS/IPS, Monitoring Systems, SIEM, etc.), Threat Vectors, and Indicators of Compromise (IOC) Overview

Objective: Analyze perimeter security systems – for example firewall, IDS/IPS, monitoring systems, and SIEM tools to develop an understanding of purpose, function, and limitations. Identify key threat vectors that may assist an organization in assessing cyber-risk to the organization. Define and explain the value of indicators of compromise (IOCs).

Course Goal Connection:
1. Obtain in-depth knowledge on various security systems examples.
2. Gain increased understanding of attack models used against security systems.
3. Learn how security systems provide defenses/countermeasures against attack vectors.

Required Reading:
- **Review**: NIST Special Publication 800-94 (February 2007) Chapter 2 and 3
- **Read**: FireEye -- M-Trends 2018 Posted on Blackboard -- AIT 671 Week 5
- **Read**: Mandiant -- M-Trends 2017 Posted on Blackboard -- AIT 671 Week 5
- **Read**: Mandiant -- M-Trends 2016 Posted on Blackboard -- AIT 671 Week 5
- **Read**: RTFM: Red Team Field Manual, CreateSpace Independent Publishing Platform; 1.0 edition (February 11, 2014), see lab materials
- **Watch**: Mandiant -- APT1: Exposing One of China’s Cyber Espionage Units -- https://www.youtube.com/watch?v=6p7FqSav6Ho
- **Watch**: Sourcefire -- Introduction to Intrusion Prevention Systems https://www.youtube.com/watch?v=2lbkG7VuNXA
- **Watch**: Sourcefire -- Intrusion Prevention System Categories https://www.youtube.com/watch?v=rP_BDCsxFxc

Other Reading (Recommended):
- Paper readings and Internet resources posted on Blackboard -- AIT 671

Week 5 Assignment:
- **Hands-on Team Activity #2 (Not graded)** – in-class activity using cyber tools and processes we have been discussing.

Week 6: Network Defense and Vulnerability Scanning

Objective: Identify four (4) network defense tools that can be deployed within an enterprise to increase visibility of potential compromised resources. Analyze IDS operations and explain results of alert activity. Analyze and explain vulnerability scanning activity and results/report output from a scan.

Course Goal Connection:
1. Obtain in-depth knowledge on various security systems examples.
2. Gain increased understanding of attack models used against security systems.
3. Learn how security systems provide defenses and counter measures against attack vectors.
4. Understand overall evaluation and management of security systems life cycle.

**Required Reading:**
- **Read:** RTFM: Red Team Field Manual, CreateSpace Independent Publishing Platform; 1.0 edition (February 11, 2014), see lab materials
- **Read:** Symantec — Internet Security Threat Report 2018
  Posted on Blackboard -- AIT 671 Week 6
- **Read:** Symantec — Internet Security Threat Report 2017
  Posted on Blackboard -- AIT 671 Week 6
- **Read:** Symantec — Internet Security Threat Report 2016
  Posted on Blackboard -- AIT 671 Week 6
- **Review:** Tenable Nessus Data Sheet
  http://www.tenable.com/resources?keys=&type_1=data_sheet
- **Review:** Tripwire IP360 Data Sheet http://www.tripwire.com/register/tripwire-ip360-datasheet/
- **Watch:** Cisco -- Cisco Intrusion Prevention System
  Link: https://www.youtube.com/watch?v=3Tvqo41Mhc0
- **Watch:** Doug Burks -- Security Onion and Sguil
  Link: https://www.youtube.com/watch?v=NV2pz07RfMQ&index=9&list=PLMN5wm-C5YjyieO63g8LbaiWTSJRj0DBe

**Other Reading (Recommended):**
- Paper readings and Internet resources posted on Blackboard -- AIT 671

**Week 6 Assignment:**
- **Lab #2 -- in-class lab supporting cyber tools, attack vectors, network defense options and processes we have been discussing**

**Week 7: User Security Awareness/Training**

**Objective:** Compare and contrast differing opinions on the value of corporate user security awareness/training. Identify and explain three (3) benefits of user security awareness/training. Identify and explain three (3) drawbacks of user security awareness/training.

**Course Goal Connection:**
1. Obtain in-depth knowledge on various security systems examples.
2. Gain increased understanding of attack models used against security systems.
3. Understand overall evaluation and management of security systems life cycle.

**Required Reading:**
• **Read:** “Get real about user security training” InfoWorld

• **Read:** “Why you shouldn’t train employees for security awareness” CSO

• **Review:** NIST Special Publication 800-100 (March 2007) Chapters 4

• **Review** NIST Special Publication 800-53 Revision 4 (April 2013) Chapters 1 and 2 – with additional concentration on AT family

**Other Reading (Recommended):**
• Paper readings and Internet resources posted on *Blackboard* -- AIT 671

**Week 7 Assignment:**
• **Team Paper -- User Awareness/Training Debate**

**Week 8: Evaluation Methods and Metrics on Measuring Security Enhancements**

**Objective:** Develop an understanding of the different evaluation and assessment standards for security systems. Describe the benefits of measuring metrics of security systems / processes.

**Course Goal Connection:**
3. Learn how security systems provide defenses and counter measures against attack vectors.
4. Understand overall evaluation and management of security systems life cycle.

**Required Reading:**
• **Read** NIST Special Publication 800-100 (March 2007) -- Chapter 7 and 11
• **Read:** HP — Cyber Risk Report 2016 -- Posted on *Blackboard* -- AIT 671 Week 8
• **Read:** RTFM: Red Team Field Manual, CreateSpace Independent Publishing Platform; 1.0 edition (February 11, 2014), see lab materials
• **Review:** Akamai Whitepaper: UPnPProxy: Blackhat Proxies via NAT Injections (2018) -- Posted on *Blackboard* -- AIT 671 Week 8
• **Review:** DHS, Continuous Diagnostics and Mitigation (CDM) -- [http://www.dhs.gov/cdm](http://www.dhs.gov/cdm)
• **Review:** Center for Internet Security, *The Critical Security Controls for Effective Cyber Defense Version 7*
• **Review:** ISACA, Control Objectives for Information and Related Technology (COBIT) 5 open source information -- [http://www.isaca.org/COBIT/Pages/default.aspx](http://www.isaca.org/COBIT/Pages/default.aspx)
• **Review** NIST Special Publication 800-115 (September 2008)
  Technical Guide to Information Security Testing and Assessment
• **Review** NIST Special Publication 800-53 Revision 5 (2017) Chapters 1 and 2 – with additional concentration on CA and RA families
• **Preview:** ISO/IEC 27001 - Information security management

**Other Reading (Recommended):**
• Paper readings and Internet resources posted on *Blackboard* -- AIT 671

**Week 8 Assignment:**
• **Lab #3 -- in-class lab supporting cyber tools, attack vectors, network defense options and processes we have been discussing**
Week 9: Physical Security and Business/Disaster Recovery

Objective: Analyze physical security incidents to develop an understanding of the critical requirement for physical security on cyber assets and systems. Identify the three different disaster recovery sites and pros/cons for selecting each type of site.

Course Goal Connection:
1. Obtain in-depth knowledge on various security systems examples.
2. Gain increased understanding of attack models used against security systems.
3. Learn how security systems provide defenses and counter measures against attack vectors.
4. Understand overall evaluation and management of security systems life cycle.

Required Reading:
- **Read:** USA Today, “FBI investigating 11 attacks on San Francisco-area Internet lines” http://www.usatoday.com/story/tech/2015/06/30/california-internet-outage/29521335/
- **Read:** Analysis of the Cyber Attack on the Ukrainian Power Grid (March 2016) – Week 9 materials

Other Reading (Recommended):
- Paper readings and Internet resources posted on Blackboard -- AIT 671

Week 9 Assignment:
- **Current Cyber Event Paper #2**

Week 10: Client-side Security

Objective: Identify four (4) common client-side cyber vulnerabilities. Describe four (4) client-side defensive security controls that can be implemented to reduce the cyber risk of client-side vulnerabilities to an organization. Describe a zero day (0-day) with regards to software and the risk these pose to corporations. Explain whitelisting with regards to cyber defensive control.

Course Goal Connection:
1. Obtain in-depth knowledge on various security systems examples.
2. Gain increased understanding of attack models used against security systems.
3. Learn how security systems provide defenses and counter measures against attack vectors.
4. Understand overall evaluation and management of security systems life cycle.

Required Reading:
• **Read:** AUSTRALIAN SIGNALS DIRECTORATE (ASD), "Essential Eight Explained" (February 2017)
  (Also -- view supporting video)
• **Read:** AUSTRALIAN SIGNALS DIRECTORATE (ASD), “‘Top 4’ Strategies to Mitigate Targeted Cyber Intrusions “ (July 2013)
• **Read** Ransomware Executive One-Pager -- Posted on Blackboard -- AIT 671 Week 10
• **Read** Ransomware Prevention and Response for CISOs --
  Posted on Blackboard -- AIT 671 Week 10
• **Read** Ransomware Locky (IAD Operational Fusion and Analysis Publication)
  Posted on Blackboard -- AIT 671 Week 10
• **Review:** Social-Engineer.org, --"Social Engineering Capture the Flag Results" Defcon 19
• **Review:** Microsoft Enhanced Mitigation Experience Toolkit (EMET)
• **Review:** NIST Special Publication 800-167 Guide to Application Whitelisting (2015) --
  https://csrc.nist.gov/publications/detail/sp/800-167/final
• **Watch:** OWASP AppSecUSA 2014, “When you can’t afford 0days: Client-side exploitation for the masses - OWASP AppSecUSA 2014”
  Link: https://www.youtube.com/watch?v=BmQawZVF9HY
• **Watch:** DEF CON 22, “DEF CON 22- David Wyde - Client-Side HTTP Cookie Security: Attack and Defense” -- Link: https://www.youtube.com/watch?v=tso5rhzQYBc
• **Watch:** CORE Impact, “CORE Impact Client Side Testing”
  Link: https://www.youtube.com/watch?v=rNgAW95LQEM

**Other Reading (Recommended):**
• Paper readings and Internet resources posted on Blackboard -- AIT 671

**Week 10 Assignment:**
• **Hands-on Team Activity #3 (Not graded)** -- in-class activity using cyber tools and processes we have been discussing.

**Week 11: Cybersecurity Manager Introduction to “Offense” (Pen Testing, Red Team, Auditing)**

**Objective:** Develop an understanding of common threat vectors used in offensive cyber-attacks. Identify three (3) common threat vectors. Explain the difference between threat, vulnerability, exploitation, and exfiltration with regards to cyber-attacks. Explain the value of pen testing and/or auditing with respect to leadership within a corporation.

**Course Goal Connection:**
2. Gain increased understanding of attack models used against security systems.
3. Learn how security systems provide defenses and counter measures against attack vectors.
4. Understand overall evaluation and management of security systems life cycle.

**Required Reading:**
• **Read:** RTFM: Red Team Field Manual, CreateSpace Independent Publishing Platform; 1.0 edition (February 11, 2014), see lab materials
Read: FireEye -- "APT28 Targets Hospitality Sector, Presents Threat to Travelers « Threat Research Blog" (August 2017)
https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html

Read: FireEye -- "APT28 AT THE CENTER OF THE STORM RUSSIA STRATEGICALLY EVOLVES ITS CYBER OPERATIONS " (January 2017)


Read: ComputerWeekly, “How to use red teaming to find real-world vulnerabilities”

Read: Infosec Island, "The Five Most Important Reasons to Perform Network Auditing"


Read: “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation” -- Operational Profile of An Advanced Cyber Intrusion pg 59

Read: CSO Online, “Red Team Versus Blue Team: How to Run an Effective Simulation”

http://www.counciloncybersecurity.org/workforce/workforce-management

Other Reading (Recommended):
- Paper readings and Internet resources posted on Blackboard -- AIT 671

Week 11 Assignment:
- Lab #4 – in-class lab supporting cyber tools, attack vectors, network defense options and processes we have been discussing

Week 12: Malware against Security Systems (Software Vulnerability Attacks and Analysis)

Objective: Explain what malware is and why it can be a risk to corporations. Describe a zero day (0-day) with regards to software and the risk these pose to corporations. Identify three (3) defensive security controls that can be deployed within an organization to reduce the risk of common malware operating on a corporate network.

Course Goal Connection:
1. Obtain in-depth knowledge on various security systems examples.
2. Gain increased understanding of attack models used against security systems.
3. Learn how security systems provide defenses and counter measures against attack vectors.

Required Reading:
- Read: Mandiant, “AN OUNCE OF PREVENTION Integrating Application Security into the Software Development Lifecycle “ (January 2014)

- Read: FireEye, “Poison Ivy: Assessing Damage and Extracting Intelligence“ (August 21, 2013)
Read: Dark Reading, “Hacking Team 0-Day Shows Widespread Dangers Of All Offense, No Defense“ (July 8, 2015)  
Read: AlienVault, “BEGINNER’S GUIDE to Open Source Intrusion Detection Tools“ (July 8, 2015)  
https://doi.org/10.6028/NIST.SP.800-70r4  
Link: https://www.youtube.com/watch?v=KFx4lhxMi-M  

Other Reading (Recommended):  
- Paper readings and Internet resources posted on Blackboard -- AIT 671 - Online Course  

Week 12 Assignment:  
- Team Breakout – Status and continue work in support of Final Team Reports and Presentations  

Week 13: Common Attack Models against Security Systems  
Objective: Describe at least three (3) attack models (vectors) that are have been used against corporations within the past twelve (12) months. Explain the terms threat, vulnerability, risk, and security control with regards to cyber risk to an organization.  

Course Goal Connection:  
1. Obtain in-depth knowledge on various security systems examples.  
2. Gain increased understanding of attack models used against security systems.  
3. Learn how security systems provide defenses and counter measures against attack vectors.  
4. Understand overall evaluation and management of security systems life cycle.  

Required Reading:  
- Read: Social-Engineer.org, --“Social Engineering Capture the Flag Results” Defcon 19  
- Read: Cisco 2018 Annual Security Report – see Week 12 materials  
- Read: Cisco 2017, 2016, 2015, and 2014 Annual Security Reports – see Week 12 materials  
- Review: OWASP -- Top Ten Project - 2017  
http://cwe.mitre.org/top25/  
- Watch: Black Hat, “From Attacks to Action - Building a Usable Threat Model to Drive Defensive Choices” -- Link: https://www.youtube.com/watch?v=TANVAco3am4  

Other Reading (Recommended):  
- Paper readings and Internet resources posted on Blackboard -- AIT 671  

Week 13 Assignment:  
- Lab #5 – in-class lab supporting cyber tools, attack vectors, network defense options and processes we have been discussing  

Team Project Delivery/Presentation  

Week 14: Team Reports and Presentations
Honor Code:
All work performed in this course will be subject to the GMU’s [Honor Code](#). Any violation will be reported to the honor committee.

Academic Integrity:
GMU is an Honor Code university; please see the [Office for Academic Integrity](#) for a full description of the code and the honor committee process. The principle of academic integrity is taken very seriously and violations are treated gravely. What does academic integrity mean in this course? Essentially this: when you are responsible for a task, you will perform that task. When you rely on someone else’s work in an aspect of the performance of that task, you will give full credit in the proper, accepted form. Another aspect of academic integrity is the free play of ideas. Vigorous discussion and debate are encouraged in this course, with the firm expectation that all aspects of the class will be conducted with civility and respect for differing ideas, perspectives, and traditions. When in doubt (of any kind) please ask for guidance and clarification.

Office of Disability Services:
If you are a student with a disability and you need academic accommodations, please see me and contact the [Office for Disability Services](#) (ODS) at 993-2474, [https://ods.gmu.edu/](https://ods.gmu.edu/). All academic accommodations must be arranged through the ODS.

Mason e-mail Accounts:
_Students must use their MasonLIVE email account to receive important University information, including messages related to this class. See [https://masonlive.gmu.edu/](https://masonlive.gmu.edu/) for more information._

Other Useful Campus Resources:
**Writing Center:** A114 Robinson Hall; (703) 993-1200; [https://writingcenter.gmu.edu/](https://writingcenter.gmu.edu/)

**University Libraries “Ask a Librarian”:** [https://library.gmu.edu/mudge/IM/IMRef.html](https://library.gmu.edu/mudge/IM/IMRef.html)

**Counseling And Psychological Services (CAPS):** (703) 993-2380; [https://caps.gmu.edu/](https://caps.gmu.edu/)

**University Policies:** The University Catalog, [https://catalog.gmu.edu/](https://catalog.gmu.edu/), is the central resource for university policies affecting student, faculty, and staff conduct in university academic affairs. Other policies are available at [https://universitypolicy.gmu.edu/](https://universitypolicy.gmu.edu/). All members of the university community are responsible for knowing and following established policies.