Course Approval Form

Action Requested:
- Create new course [X]
- Delete existing course [ ]
- Modify existing course [ ]

Course Level:
- Undergraduate [ ]
- Graduate [X]

College/School: VSE (Volgenau School of Engineering)  Department: ECE
Submitted by: Robert Osgood  Ext: 3-5443  Email: rosgood@gmu.edu

Effective Term: [X] Fall  [ ] Spring  [ ] Summer  Year: 2015

Subject Code: CFRS  Number: 730
Title: Forensic Deep Packet Inspection

Credits: (check one) [X] Fixed [ ] Variable
Repeat Status: (check one) [X] Not Repeatable (NR) [ ] Repeatable within degree (RD) [ ] Repeatable within term (RT)

Grade Mode: (check one) [X] Regular (A, B, C, etc.) [ ] Satisfactory/No Credit [ ] Special (A, B C, etc. +IP)
Schedule Type Code(s): (check all that apply) [X] Lecture (LEC) [X] Lab (LAB) [ ] Recitation (RCT) [ ] Internship (INT)
[ ] Seminar (SEM) [ ] Studio (STU)

Prerequisite(s): CFRS 660
Corequisite(s): 

Instructional Mode: [X] 100% face-to-face
[ ] Hybrid: ≤ 50% electronically delivered
[ ] 100% electronically delivered

Special Instructions: (list restrictions for major, college, or degree; hard-coding; etc.)

Are there equivalent course(s)? [X] Yes [ ] No

Catalog Copy for NEW Courses Only (Consult University Catalog for models)

Description (No more than 60 words, use verb phrases and present tense) 

Notes (List additional information for the course) 

Indicate number of contact hours:
When Offered: (check all that apply) [X] Fall  [ ] Summer  [X] Spring

Hours of Lecture or Seminar per week:
Hours of Lab or Studio:

Approval Signatures

Robers Osgood 2/10/14
Department Approval Date
College/School Approval Date

If this course includes subject matter currently dealt with by any other units, the originating department must circulate this proposal for review by those units and obtain the necessary signatures prior to submission. Failure to do so will delay action on this proposal.

Unit Name
Unit Approval Name
Unit Approver’s Signature Date

For Graduate Courses Only

Graduate Council Member
Provost Office
Graduate Council Approval Date

For Registrar Office’s Use Only: Banner ________________________________ Catalog ________________________________ revised 2/2/10
1. CATALOG DESCRIPTION
   (a) CFRS 730 (3:3:0) Forensic Deep Packet Inspection
   (b) Prerequisites: CFRS 660
   (c) Catalog Description: Presents tools, techniques, and methodologies used to conduct deep packet forensic analysis. Application of industry best practices to both the collection and subsequent analysis of network packets with an emphasis on hands-on exercises using digital analysis tools.

2. JUSTIFICATION
   (a) Course Objectives:
       This course will familiarize students with the practice network forensic packet capture analysis, and specifically Deep Packet Inspection.

   (b) Course Necessity:
       The Network Forensics Deep Packet Inspection course is for students who have limited experience with the practice of packet capture forensics. Deep Packet Inspection looks at packets and tries to make some inferences about what the packets contain. For instance are these packets apart of a Command and Control server, do these packets beacon to a home base? This type of analysis is geared toward capturing the behavioral aspects of the malicious network attacks in a controlled environment. The course builds upon the core MS in Computer Forensics course CFRS 660 Network Forensics and is a critical element in advanced forensics analysis, both in the field and in the lab. As such, it will strengthen the capabilities of MS in CFRS student and enhance their employment options.

   (c) Relationship to Existing Courses:
       This course builds on the core course CFRS 660 Network Forensics. There are other applicable courses in the MS in Computer Forensics program (e.g. CFRS 663 Operation of Intrusion Detection for Forensics, and CFRS 664 Incident Response Forensics)that would also provide some elements of use in CFRS 730. As such, CFRS 730 is a new course that does not overlap to any significant degree with existing graduate courses.

3. APPROVAL HISTORY
   ECE Department Date:
   IT&E Graduate Committee Date:

4. SCHEDULING
   The course will be offered every fall and spring semester, starting fall 2014 and every regular semester thereafter.

5. COURSE OUTLINE
   (a) Syllabus
       Week 1
       Introduction & Reconnaissance - What will this class cover. What does your network reveal?

       Week 2
       Packet Carving - GUI vs. Command Line, and netcat

       Week 3
       Tools I - tshark

       Week 4
       Tools II - tcpflow, tcpdump, tcpxtract

       Week 5
       DNS Record Manipulation

       Week 6
       Obfuscation

       Week 7
       Encrypted Web Traffic

       Week 8
       Mid-Term Exam
Week 9
Network Tunneling

Week 10
Command and Control Communication

Week 11
nmap scanning

Week 12
scripting for packet carving

Week 13
PCAP Challenges - Solving forensic challenges

Weeks 14
PCAP Challenges - Solving forensic challenges

Week 15
Final Exam

Required Reading and Reference Material

Required Text:

Title: Network Forensics: Tracking Hackers through Cyberspace
Author: Sherri Davidoff, Jonathan Ham
Publisher: Prentice Hall
ISBN-10: 0-13-256471-8

Student Evaluation Criteria

<table>
<thead>
<tr>
<th>Component</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quizzes</td>
<td>15%</td>
</tr>
<tr>
<td>Labs</td>
<td>25%</td>
</tr>
<tr>
<td>Midterm</td>
<td>30%</td>
</tr>
<tr>
<td>Final Project</td>
<td>30%</td>
</tr>
</tbody>
</table>