ANEXA 2

Universitatea Politehnica Timişoara
Centrul de Educație Permanentă

Fişa disciplinei:

" Virusologie și vulnerabilități ale sistemelor informatice"

Domeniul / Specializarea: CALCULATOARE / SECURITATEA INFORMAŢIILOR ŞI A SISTEMELOR CIBERNETICE

Anul I / Semestrul II

Titularul cursului: *Conf.dr.ing. Lucian PRODAN*					
Colaboratori*: S.l.dr.ing. Alexandru IOVANOVICI*					
Număr de ore total/Verificarea/Credite					
Curs	**Seminar**	**Laborator**	**Proiect**	**Examinare**	**Credite**
21	**-**	**5**	**16**	**E**	**3**

A. Obiectivele cursului

- Extinderea cunoştinţelor teoretice în ceea ce privește amenințările moderne care planează în permanență asupra sistemelor informatice (servere, calculatoare personale, dispozitive mobile si interconectate);
- Formarea unor abilități și deprinderi de a reacționa și a lua decizii potrivite în situații care implică aspecte etice problematice;
- Înțelegerea unor aspecte de inginerie socială care fac posibilă penetrarea sistemelor informatice;
- Analiza unor tehnici de bază referitoare la virușii informatici și extinderea către conceptul de malware;
- Identificarea unor vulnerabilități la nivel de sistem de operare și la nivel de aplicație;
- Interacțiunea directă cu exemple de malware în vederea detectării, identificării și neutralizării.

B. Subiectele cursului

1. Introducere în conceptele și practica malware (6 ore)
   1.1. Noțiuni elementare despre virușii informatici
   1.2. Asemănări și deosebiri virus – troian
   1.3. RAT - Remote Access Tools
   1.4. Vulnerabilități legate de aplicații. Exemple legate de microsoft Office.
   1.5. Furtul de date (Data Stealer, Keylogger)
   1.6. Propagarea virușilor și a viermilor (worms)
   1.7. Dobândirea de drepturi prin exploatarea unor vulnerabilități. Conceptele rootkit și back-door.
   1.8. Reclame pe internet și vulnerabilități. Adware.

2. Vulnerabilități în sistemele informatice (6 ore)
   2.1. Tipuri de vulnerabilități (umane, procedurale, tehnice)
   2.2. Conceptul RAT (Remote Access Trojan)
   2.3. Vulnerabilități hardware: Intel Spectre, Meltdown, Foreshadow)
   2.4. Vulnerabilități ale sistemelor de operare: Microsoft Windows
   2.5. Vulnerabilități software (de aplicație)

3. Malware: distribuție și implementare (4 ore)
   3.1. Strategia unui atac malware. Stagiile unui atac: intrarea, distribuirea traficului, exploatarea unei vulnerabilități, infectarea, execuția de cod.

3.2. Malware multi-stage: dropper si payload.
3.3. Comunicarea cu Centrele de Comanda si Control (C&C, C2).
3.4. Tipologii atacuri cu malware: APT (Advanced Persistent Threat), Phishing / Spear-Phishing, Watering Hole, man-in-the-middle (client-server)

4. Analiza și contramăsuri malware (5 ore)
4.1. Recomandări de igiena cibernetică
4.2. Analiza statică: scanare și reverse-engineering
4.3. Analiza dinamică: rulare în sand-box, resource monitor (procese, scriere pe disk, utilizare regiștri), rulare in debugger (IDA Pro, ResourceHacker), analiza de trafic (WireShark)
4.4. Lista vulnerabilităților documentate https://cve.mitre.org

C. Subiectele aplicaţiilor (laborator, seminar, proiect)

Laborator / proiect:

1. Instalarea, configurarea și utilizarea unei mașini virtuale VMware în combinație cu Windows XP și Windows 7. Exploatarea acestora pentru depășirea parolei. Discuții asupra acestor vulnerabilități. (6 ore)
2. Procese si drepturi in Windows XP și Windows 7. Escaladarea drepturilor. Vulnerabilități ale browser-elor, buffer/heap overflow, atacuri de tip return-to-libc. (6 ore)
3. Aspecte practice legate de utilizarea sistemelor anti-virus. Analiza comportamentului unui virus care afectează dispozitivele de stocare USB (autorun.inf). (4 ore)
4. Studiu de caz. Modul de infectare, acțiune, identificare și neutralizarea unui virus. (5 ore)

D. Bibliografie

1. A.K. White. Hacking: The Underground Guide to Computer Hacking, Including Wireless Networks, Security, Windows, Kali Linux and Penetration Testing. CreateSpace Independent Publishing Platform, ISBN: 1979881103, 2017.
2. W.A. Conklin, G. White, C. Cothren, R.L. Davis, D. Williams. Principles of Computer Security, 4th Edition, McGraw-Hill Education, 2016.
3. Frederick B. Cohen. A Short Course on Computer Viruses. ASP Press, ISBN 1-878109-01-4, 1990.

E. Evaluarea

Examen scris + prezentare proiect aplicativ pe calculator
Nota finală este compusă din media celor două note obţinute: nota la examenul scris şi nota obţinută la evaluarea proiectului aplicativ.

Data: 05.09.2018

Director de program de studii postuniversitare,

Prof. dr. ing. Bogdan GROZA

Titular de disciplină,

Conf. dr. ing. Lucian PRODAN