

**BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI**

**WORK INTEGRATED LEARNING PROGRAMMES**

**COURSE HANDOUT**

**Part A: Content Design**

|  |  |
| --- | --- |
| **Course Title** | **Ethical Hacking** |
| **Course No(s)** | **SS ZG575** |
| **Credit Units** | **4** |
| **Credit Model** | **4 (1: Class Room Hours; 2: Students Preparation; 1: Lab Work/Case Studies)**  ***(1 credit unit translates to approximately 32 hours)*** |
| **Course Authors** | **Prof. G Geethakumari** |
| **Version No** | **1** |
| **Date** | **April 30, 2020** |

**Course Objectives**

|  |  |
| --- | --- |
| **No** | **Course Objective** |
| **CO1** | Introduce students to the techniques and tools for ethical hacking and countermeasures |
| **CO2** | To develop skills of exploit approaches – social engineering, scanning, foot-printing, enumeration, sniffers, buffer overflows |
| **CO3** | Understand service-specific hacking like DNS, Email, Web servers, Proxy; techniques of bypassing security mechanisms and hardening systems and networks for countermeasures of security analysis, monitoring and analysis tools including network traffic and system logs |
| **CO4** | Also learn the security paradigms in cloud computing, mobile platforms and online social networks. |

**Text Book(s)**

|  |  |
| --- | --- |
| T1 | Stuart McClure, Joel Scambray, George Kurtz, “Hacking Exposed 7: Network Security Secrets and Solutions, TMGH 2012 |

**Reference Book(s) & other resources**

|  |  |
| --- | --- |
| R1 | Joseph Muniz, Aamir Lakhani, “Web Penetration Testing with Kali Linux”, Shroff 2013 |
| R2 | Nipun Jaiswal, “Mastering Metasploit”, Shroff/Packt 2014 |
| R3 | Neil Bergman etc. “Hacking Exposed Mobile: Security Secrets & Solutions”, MGH 2013 |

#### Online References

|  |  |
| --- | --- |
| O1 | https://www.owasp.org/index.php/Category:OWASP\_Top\_Ten\_Project |
| O2 | https://www.stateoftheinternet.com/ |
| O3 | http://www.symantec.com/security\_response/publications/threatreport.jsp |
| O4 | http://www.kb.cert.org/vuls |
| O5 | http://googleprojectzero.blogspot.in |
| O6 | https://code.google.com/p/google-security-research/issues/list |
| O7 | https://source.android.com/security/index.html and sublinks |

**Modular Content Structure**

1. Introduction to Ethical Hacking
   1. Objective of the course
   2. Service, Application, Device, System, Person; Lifecycle for attack
   3. Understand trust boundaries; Use cases and discussions
2. Basics of tools and techniques for Ethical hacking
   1. Root-kits, covert-channels, sniffing, MITM, botnets
   2. Covering the traces, Camouflage, Defeat forensics
   3. Understand trust boundaries; Use cases and discussions
3. Vulnerabilities and Reverse engineer binaries
   1. Vulnerability Identification and Assessment
   2. Binary Auditing, runtime tracing, log analysis
   3. Disassembling, firmware, application, shared objects
4. Mobile applications security
   1. Mobile Hacking, Android Security – kernel, application and updates
   2. File system level access, Jailbreak, super-user, rootkits, MITM
   3. Countermeasures: Strategies, Scenarios
5. Casing the Establishment
   1. Foot-printing
   2. Scanning
   3. Enumerating
   4. DNS, Sniffing, DHCP ; Non-invasive survey of application and devices
6. Wireless Hacking and Hacking Hardware
   1. Wireless hacking
   2. Protocols, Sniffers, Re-play, Man-in-the-middle
   3. Router / Access-point compromise: Physical access, Reverse engineering hardware
7. Remote Connectivity and VoIP
   1. Special strategies to compromise VoIP end device
   2. VoIP server/proxy
   3. VPN server
8. Security Issues on Web server and Databases
   1. Exploiting in Web Server
   2. Databases
   3. Cloud Infrastructure
9. Processes and tools used for Defense
   1. Defense, general strategies, Honeypots
   2. IDS/IPS designs, exceptions
10. Recent hack reports
    1. Review of recent Vulnerabilities and tools
    2. Recap of the course in perspective of current events

**Learning Outcomes:**

|  |  |
| --- | --- |
| **No** | **Learning Outcomes** |
| LO1 | Understand the components of enterprise and consumer applications and systems that can be exploited for hacking. |
| LO2 | Use tools and techniques to survey the target in the cyber world using foot printing, scanning and enumerating. |
| LO3 | Learn about multiple approaches to find vulnerabilities and exploit them using (a) network based attacks (b) host level compromise across different platforms and (c) deployment / system-component level attacks. |
| LO4 | Understand the weaknesses in wireless communications and execute some of the exploits in controlled environment. |
| LO5 | Learn about tools to defend against attacks or minimize the damage. |

**Part B: Course Handout**

|  |  |
| --- | --- |
| **Academic Term** | Second Semester 2020-2021 |
| **Course Title** | Ethical Hacking |
| **Course No** | SS ZG575 |
| **Lead Instructor** | JAGDISH PRASAD |

|  |  |  |  |
| --- | --- | --- | --- |
| **Session No.** | **List of Topic Title**  **(from content structure in Part A)** | **Topic #**  **(from content structure in Part A)** | **Text/Ref Book/external resource** |
| 1 | Introduction to Ethical Hacking | Objective of the course  Service, Application, Device, System, Person; Lifecycle for attack; Understand trust boundaries; Use cases and discussions | Lecture notes  O1, O2, O3 |
| 2 | Basics of tools and techniques for Ethical hacking | Root-kits, covert-channels, sniffing, MITM, botnets, Covering the traces, Camouflage, Defeat forensics, Understand trust boundaries; Use cases and discussions | Class Notes |
| 3 | Vulnerabilities and Reverse engineer binaries | Vulnerability Identification and Assessment | O4 and Class notes |
| 4 | Vulnerabilities and Reverse engineer binaries | Binary Auditing, runtime tracing, log analysis, Disassembling, firmware, application, shared objects | O5, O6 and Class notes |
| 5 | Mobile applications security | Mobile Hacking, Android Security – kernel, application and updates;  File system level access, Jailbreak, super-user, rootkits, MITM  Countermeasures: Strategies, Scenarios | O7 with subsections and T1: 11,12 |
| 6 | Casing the Establishment | Foot-printing, Scanning | T1: 1,2 |
| 7 | Casing the Establishment | Enumerating, DNS, Sniffing, DHCP ; Non-invasive survey of application and devices | T1: 3,  Class notes |
| 8 | Wireless Hacking and Hacking Hardware | Wireless hacking | T1: 8 |
| 9 | Wireless Hacking and Hacking Hardware | Protocols, Sniffers, Re-play, Man-in-the-middle, Router / Access-point compromise: Physical access, Reverse engineering | T1: 9  Class notes |
| 10 | Remote Connectivity and VoIP | Special strategies to compromise VoIP end device, VoIP server/proxy, VPN server | T1: 7 |
| 11 | Security Issues on Web server and Databases | Exploiting in Web Server | T1:10;O:1 |
| 12 | Security Issues on Web server and Databases | Exploiting in Databases, Cloud Infrastructure | T1:10;O:1,  Class notes |
| 13 | Processes and tools used for Defense | Defense, general strategies, Honeypots | O1, Class notes |
| 14 | Processes and tools used for Defense | IDS/IPS designs, exceptions | O1, Class notes |
| 15-16 | Recent hack reports | Review of recent Vulnerabilities and tools, Recap of the course in perspective of current events | Class notes |

**Detailed Plan for Lab work/Design work**

|  |  |
| --- | --- |
| **Lab No.** | Topics |
| 1 | Understanding the lab setup, isolated network, remote shell and related network protocols |
| 2 | Compilers, assemblers, disassemblers, debuggers, trace tools, environment, sniffers etc. |
| 3 | Linux password cracking exercises – different encryptions |
| 4 | Reverse engineering a firmware update |
| 5 | Android tools, app development, and hacking an application to embed our code |
| 6 | Executing OS exploits – Linux |
| 7 | Executing OS exploits – Windows |
| 8 | Understand tools in Kali Linux for survey attempts |
| 9 | Executing protocol exploits – Web Server and Data Bases |
| 10 | Trojans and Camouflage |
| 11 | Wireless Hacking – HackRF One |
| 12 | Tools to mine online social information |
| 13 | Defense – Audit, discover and limit, detect malware, Honeypots, Firewalls, IDS/IPS, Log service |
| 14 | Mock capture the flag exercise |

**Case studies: Detailed Plan**

|  |  |  |
| --- | --- | --- |
| **Case study No** | **Case study Objective** | **Case study Sheet Access URL** |
| - | - | - |

**Evaluation Scheme**:

Legend: EC = Evaluation Component; AN = After Noon Session; FN = Fore Noon Session

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Name | Type | Duration | Weight | Day, Date, Session, Time |
| EC-1 | Quiz-I | Online | - | 5% | February 1-15, 2021 |
|  | Quiz-II | Online | - | 5% | March 1-15, 2021 |
|  | Assignment / Lab | Offline | - | 10% | April 1-15, 2021 |
| EC-2 | Mid-Semester Test | Closed Book | 1.5 hours | 30% | Saturday, 06/03/2021 (AN)  2 PM – 4 PM |
| EC-3 | Comprehensive Exam | Open Book | 2.5 hours | 50% | Saturday, 01/05/2021 (AN)  2 PM – 5 PM |

**Note: If Assignment kindly remove Quiz-I, II, III**

Syllabus for Mid-Semester Test (Closed Book): Topics in Sessions/Contact Hours :8 (or)1 to 16 hours

Syllabus for Comprehensive Exam (Open Book): All topics (Session Nos. 1 to 16 (or) 1 to 32 hours)

**Important links and information:**

Elearn portal: https://elearn.bits-pilani.ac.in

Students are expected to visit the Elearn portal on a regular basis and stay up to date with the latest announcements and deadlines.

Contact sessions: Students should attend the online lectures as per the schedule provided on the Elearn portal.

Evaluation Guidelines:

1. EC-1 consists of an Assignment and two Quizzes. Students will attempt them through the course pages on the Elearn portal. Announcements will be made on the portal, in a timely manner.
2. For Closed Book tests: No books or reference material of any kind will be permitted.
3. For Open Book exams: Use of books and any printed / written reference material (filed or bound) is permitted. However, loose sheets of paper will not be allowed. Use of calculators is permitted in all exams. Laptops/Mobiles of any kind are not allowed. Exchange of any material is not allowed.
4. If a student is unable to appear for the Regular Test/Exam due to genuine exigencies, the student should follow the procedure to apply for the Make-Up Test/Exam which will be made available on the Elearn portal. The Make-Up Test/Exam will be conducted only at selected exam centres on the dates to be announced later.

It shall be the responsibility of the individual student to be regular in maintaining the self study schedule as given in the course handout, attend the online lectures, and take all the prescribed evaluation components such as Assignment/Quiz, Mid-Semester Test and Comprehensive Exam according to the evaluation scheme provided in the handout.