Uka Tarsadia University

M.Sc. (C.A.)

Penetration Testing (040020305)

3rd Semester

EFFECTIVE FROM JUNE-2012

Uka Tarsadia University

MSc(CA) (3rd Semester) Syllabus, June 2012

Prerequisite: Knowledge of computer network and web.

Aim and Objective: Provide Understanding of penetration testing.

Subject Code: 040020305 **Subject:** Penetration Testing

Total: 48 [Lecture:4 Tutorial:0 Practical: 0]

1. Beginning with BackTrack [08 Hrs.]

1.1 BackTrack purpose
1.2 Getting and Using BackTrack
1.3 Configuring network connection
1.4 Updating and Customizing BackTrack
1.5 Types of penetration testing
1.6 Vulnerability assessment versus penetration testing
1.7 Security testing methodologies
1.8 BackTrack testing methodology

2. Target Scoping and Information Gathering [08 Hrs.]

2.1 Gathering client requirements
2.2 Preparing the test plan
2.3 Profiling test boundaries
2.4 Defining business objectives, Project management and
2.5 Public resources and Document gathering
2.6 DNS and Route information, Utilizing search engines
2.7 All-in-one intelligence gathering
2.8 Documenting the information

3. Target Discovery and Enumerating [08 Hrs.]

3.1 Introduction
3.2 Identifying the target machine
3.3 OS fingerprinting
3.4 Port scanning
3.5 Service enumeration
3.6 VPN enumeration

4. Vulnerability Mapping and Social Engineering [08 Hrs.]

4.1 Types of vulnerabilities, Vulnerability taxonomy
4.2 Open Vulnerability Assessment System (OpenVAS)
4.3 Cisco analysis, Fuzzy analysis, SMB analysis, SNMP analysis
4.4 Web application analysis, Application assessment tools
4.5 Modeling human psychology, Attack process and methods
4.6 Social Engineering Toolkit (SET)
4.7 Common User Passwords Profiler (CUPP)

5. Target Exploitation and Privilege Escalation [08 Hrs.]

5.1 Vulnerability research
5.2 Vulnerability and exploit repositories
5.3 Advanced exploitation toolkit
5.4 Target Exploitation Summary
5.5 Attacking the password
5.6 Network sniffers
5.7 Network spoofing tools
5.8 Privilege Escalation Summary

6. Maintaining Access, Documentation and Reporting [08 Hrs.]

6.1 Protocol tunneling
6.2 Proxy
6.3 End-to-end connection
6.4 Documentation and results verification
6.5 Types of reports
6.6 Presentation
6.7 Post testing procedures

MODES OF TRANSCATION (i.e. Delivery)

Various methods of teaching could be employed depending on the objectives of the content taught.

- Lecture method is recommended along with discussion method.
- Activity assignment may be given to the students in group.
- Case study can be used to teach in-depth.

Teachers Activities/Practicum:

The following activities should be carried out by the teachers.

1. Simulation/Demonstration of Vulnerability Scanner.
2. Ethical Hacking related demonstration.

Student Activities/Practicum:

The following activities may be carried out by the students.

1. History and Recent Development in Back Tracking.
2. Related Professional Certification.
3. Analyze test network and prepare documentation.

[Weightage to be given in Continuous Internal Evaluation]

Text Book:

1. Tedi Heriyanto,Shakeel Ali (2011). Backtrack 4: Assuring Security By Penetration Testing, Shroff/Packt Publishing.

Reference Books:

1. Vivek Ramachandran. BackTrack 5 Wireless Penetration Testing Beginner's Guide, Shroff/Packt Publishing.
2. Lee Allen. Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide, Shroff/Packt Publishing.
3. Patrick Engebretson. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy, Syngress.
4. Ronald L. Krutz and Russell Dean Vines. The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking, Wiley
5. Thomas Wilhelm. Professional Penetration Testing: Volume 1: Creating and Learning in a Hacking Lab, Syngress