**BCY233T04 ETHICAL HACKING**

**Common for B.Sc. (CS) / BCA/B.Sc. (Data Science)/B.Sc. (Cyber security)**

**COURSE OBJECTIVES**

· To know the theory and practices of finding the vulnerabilities.

· To find the different attacks and then defining the appropriate security policy.

· To take action to detect or prevent the attacks and thus reduce the damages.

· To understand the concept of Web Server Hacking.

· To understand the concept of Firewalls

**COURSE OUTCOMES:**

· To describe the basics of the ethical hacking.

· Ability to learn technical foundations of hacking.

· Able to perform the foot printing and scanning.

· Demonstrate the techniques for system hacking.

· Characterize the malware and their attacks.

**SYLLABUS**

**UNIT – I INTRODUCTION TO ETHICAL HACKING**

Security Fundamental - Security Testing - Hacker and Cracker – Descriptions - Test Planskeeping

it legal - Ethical and Legality- Process - The Ethical Hacker’s Process.

**UNIT – II FOOTPRINTING AND SCANNING**

Information Gathering - Determining the Network Range - Finding Open Ports and Access

Points - OS Fingerprinting Services - Mapping the Network Attack Surface.

**UNIT – III MALWARE THREATS AND SESSION HIJACKING**

Viruses and Worms- Trojans - Covert Communication - Keystroke Logging and Spyware –

Malware Counter Measures- Sniffers - Session Hijacking - Denial of Service.

**UNIT – IV WEB SERVER HACKING AND ATTACKS**

Web Server Hacking - Web Application Hacking - Database Hacking - Wireless

Technologies – Mobile Security and Attacks: Wireless Technologies – Wireless LANs.

**UNIT – V CASE STUDY**

Intrusion Detection Systems - Firewalls - Honeypots - Physical Security - Social Engineering

– Case Studies: Intrusion detection Real Secure Tripwire Dragon Snort.

**TEXT BOOKS:**

1. Michael Gregg, “Certified Ethical Hacker”, Pearson IT Certification, 3rd Edition, 2019.

2. Roger Grimes, “Hacking the Hacker”, Wiley, 1st Edition, 2017

**REFERENCES:**

1. Ankit Fadia, “The Unofficial Guide to Ethical Hacking”, Laxmi Publications, 2nd

Edition, 2006.

2. Randy Weaver, Dawn Weaver, Dean Farwood, “Guide to Network Defense and

Countermeasures”, Cengage Learning, Third edition, 2014

**Notes**

**UNIT – I INTRODUCTION TO ETHICAL HACKING**

Security Fundamental - Security Testing - Hacker and Cracker – Descriptions - Test Planskeeping

it legal - Ethical and Legality- Process - The Ethical Hacker’s Process.

No organization can ever be 100 percent secure. There will always be some risk left over, known as residual risk,

**Ethical hacking**, also known as **penetration testing** or **white-hat hacking**, is the practice of intentionally probing computer systems, networks, or applications for security vulnerabilities by CEH — but with permission and for a good purpose, to find and fix weaknesses before malicious hackers (black-hats) can exploit them.

**Common tasks of Ethical Hacker:**

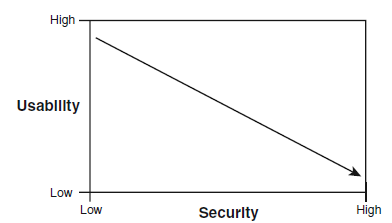
* Scanning for open ports or vulnerabilities
* Testing password strength
* Bypassing authentication mechanisms
* Exploiting vulnerabilities (safely) to demonstrate risks
* Reporting findings with recommendations

**Security Fundamentals:**

One way to secure a system from network attack is to unplug it ☺ and make it a standalone system. Although this system would be relatively secure from Internet-based attackers, its usability would be substantially reduced.

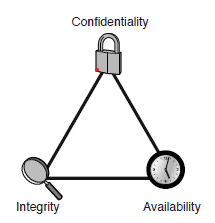
The opposite approach of plugging it in directly to the Internet without any firewall, antivirus, or security patches would make it extremely vulnerable, yet highly accessible.

So, the job of security professionals is to find a balance somewhere between security and usability.



Security triad of confidentiality, integrity, and availability (CIA) form the basic building blocks of any good security initiative.

* Confidentiality – lakhs of pwd breaches in Yahoo, Dropbox, etc
* Integrity – accuracy of same data across departments, Correctness doesn’t mean that the data is accurate, just that it hasn’t been modified in storage or transit. Integrity in electronic documents and data is much more difficult to protect than in paper ones. Electronic storage can be tightened with Cryptographic, Access control. In transit, same can be controlled with protocols.
* Availability: a legitimate user needs the information, it should be available. If no recent backups are done, there is not point to restore. Backups, SLA, Redundant Array of Inexpensive Disks(RAID), Redundant storage (Hot, Warm, Cold) can control this during Disaster management scenarios for Business Continuity (BCP)



**Risk, Assets, Threats, and Vulnerabilities:**

* Risk is the probability or likelihood of the occurrence or realization of a threat. U.S. federal government has adopted a six step risk management framework (RMF).
* An asset is any item of economic value owned by an individual or corporation like routers, servers, formula, trade secret, xls, processing time, etc.,
* A threat is an event that sets the stage for risk and is any agent, condition, or circumstance that could potentially cause harm, loss, or damage, or compromise an IT asset or data asset and can result in
  + Destruction (Natural disaster)
  + Disclosure (by hackers - An insider or outsider who is unauthorized and purposely attacks an organization’s components,
  + Cyber-attack to systems,
  + Viruses and Malware tool that do data modification, corruption of data
  + Denial of service (DoS) or Distributed DoS: To bring the network or access to a particular

TCP/IP host/server to its knees by flooding it with useless traffic.

* vulnerability is a weakness in the system design, implementation, software, or code, or the lack of a mechanism in OS, Applications, Config Files, Shrinkwrap software (ready-made, off-the-shelf software for huge common audience without custom fixes/features for specific customer. Ex: MS Office, Windows, etc)

**Backups:**

* Full: Takes longer time without excluding any files
* Differential back up: After a full back up, this is periodically done only with modified/created files, restoration done with last full and differential backup
* Incremental back up: After a full back up, this is daily done. Slow in restoration due to large number of incremental backups.

**Exploits:** An *exploit* refers to a piece of software, a tool, a technique, or a process that takes

advantage of a vulnerability that leads to access, privilege escalation, loss of integrity,

or denial of service on a computer system.

**zero-day exploit:** Sometimes you may not even know the vulnerability exists, and that is known as zero-day exploit.

**Risk Assessment:** is a process to identify potential security hazards and evaluate what would happen if a hazard or unwanted event were to occur.

Approaches to risk assessment:

* Qualitative risk assessment: methods use scenarios to drive a prioritized list of critical concerns and do

not focus on dollar amounts. Example impacts might be identified as critical, high,

medium, or low.

* Quantitative risk assessment: assigns a monetary value to the asset.

**Step 1. Determine the single loss expectancy (SLE):** involves determining the single amount of loss you could incur on an asset if a threat becomes realized or the amount of loss you expect to incur if the asset is

exposed to the threat one time. SLE is calculated as follows: SLE = asset value × exposure factor.

Step 2. **Evaluate the annual rate of occurrence (ARO):** The purpose of evaluating the ARO is to determine how often an unwanted event is likely to occur on an annualized basis.

Step 3. **Calculate the annual loss expectancy (ALE):** This final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. This is expressed as annual

loss expectancy (ALE), which is calculated as follows: ALE = SLE × ARO.

**Security testing** is the primary job of ethical hackers. These tests might be configured in such way that the ethical hackers have no knowledge, full knowledge, or partial knowledge of the target of evaluation (TOE).

* No-Knowledge Tests (Black Box)
* Full-Knowledge Testing (White Box): tester has full knowledge of the network, systems, and infrastructure.
* Partial-Knowledge Testing (Gray Box)
* Names of Security Tests:
  + Vulnerability testing
  + Network evaluations
  + Red-team exercises
  + Penetration testing
  + Host vulnerability assessment
  + Vulnerability assessment
  + Ethical hacking

Types of Security Tests:

* + **High-level assessment/audit:** Also called a level I assessment, it is a top down look at the organization’s policies, procedures, and guidelines. The purpose of a top-down assessment is to answer three questions:
    - Do the applicable policies, procedures, and guidelines exist?
    - Are they being followed?
    - Is their content sufficient to guard against potential risk?

**UNIT – II FOOTPRINTING AND SCANNING**

Information Gathering - Determining the Network Range - Finding Open Ports and Access

Points - OS Fingerprinting Services - Mapping the Network Attack Surface.

**UNIT – III MALWARE THREATS AND SESSION HIJACKING**

Viruses and Worms- Trojans - Covert Communication - Keystroke Logging and Spyware –

Malware Counter Measures- Sniffers - Session Hijacking - Denial of Service.

**UNIT – IV WEB SERVER HACKING AND ATTACKS**

Web Server Hacking - Web Application Hacking - Database Hacking - Wireless

Technologies – Mobile Security and Attacks: Wireless Technologies – Wireless LANs.

**UNIT – V CASE STUDY**

Intrusion Detection Systems - Firewalls - Honeypots - Physical Security - Social Engineering

– Case Studies: Intrusion detection Real Secure Tripwire Dragon Snort.