

ATME COLLEGE OF ENGINEERING

13th KM Stone, Bannur Road, Mysore - 560 028



A T M E

College of Engineering

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

- CYBER SECURITY



LECTURE NOTES

COURSE: ETHICAL HACKING

COURSE CODE: BCY702

SEMESTER: VII

COURSE COORDINATOR: Mr. Chetan G

(ACADEMIC YEAR 2026-27)

CHAPTER-2

Setting the Stage

HACKING IMPACTS

At the risk of stating the obvious, hacking—computer crime—can result in massive financial losses for companies, governments, and individuals alike.

The costs associated with computer crime can manifest themselves in various ways, which may range from the obscure to a clear hit to the bottom line.

Digital assets where costs from hackers can manifest themselves fall into four major categories: resources, information, time, and reputation.

1. *Resources.* Resources are computer-related services that perform actions or tasks on the user's behalf.
2. *Information.* Information can represent an enormous cost if destroyed or altered without authorization.
 - a. *Loss.* The loss of data is relatively easy to measure when compared to disclosure and integrity. Information takes time to collect or produce, requires resources to be managed, and will certainly (to some degree) have value.
 - b. *Disclosure.* Nearly every entity that uses information has the potential to be negatively affected by its uncontrolled disclosure.
 - c. *Integrity.* Ensuring information is accurate and complete is necessary for any organization. If data were to be manipulated it could become a loss to the owner. This can be as simple as the cost of an item online being \$99.99 but represented as \$9.99 because a hacker found a way of manipulating cookies to move the decimal point one position to the left.
3. *Time.* The loss of time can be related to costs in the form of payroll, not meeting critical deadlines, or an unavailable E-commerce site that would normally produce thousands of dollars in revenue if it were available.
4. *Brand and Reputation.* There are many companies who have very recognizable brands, so much so that the color alone will promote images of the company.

THE HACKER

In the early days of computing a hacker was someone who investigated the workings of computers for fun and a challenge. Cracker was a term used to identify people who would break computers to use them for free or use system resources. Somewhere between the Internet revolution and the movies, hacker was adopted to describe computer criminals.

TYPE OF HACKER

There are several types of hackers, but we can reduce this to three basic characteristics that we can use to categorize the enemy:

1. Script kiddies
2. Hackers
3. Über hacker

1. SCRIPT KIDDIES

“Script kiddie” refers to a hacker wannabe who leverages tools created by other, more knowledgeable hackers to perform malicious acts. Script kiddies can be grouped into three areas:

unstructured, structured, and determined.

- *Unstructured. This group is better defined as pranksters or a nuisance that usually includes juvenile acts that are typically not long lasting.*
- *Structured. The right tool in the wrong hands can have immense potential and combined with an opportunistic behavior can have measurable results.*
- *Determination. The persistence of an attacker certainly increases the probability of success. If for nothing other than sheer luck, a determined script kiddie will get in eventually.*

2. HACKERS

Hackers are the next step in the evolution of an attacker and make up the majority of the people who inflict chaos. Hackers explore computers for education, the challenge, and to achieve a social status among other hackers. They work diligently to obtain resources and compete with their peers to gain recognition and power within the hacking community.

There are four distinguishing faculties of the hacker: malicious, solvers, hacktivist, and vigilante. Each of these has its own unique idiosyncrasy.

- *Malicious. Malicious hackers are people with the sole intent of causing damage, destruction, or disruption of information systems. Writers of malware fall directly into this category, as do people who gain access to sites and corrupt information.*
- *Solvers. There are hackers that gain access to systems to solve a problem they or a friend may have. Many of these attacks are based on changing or removing information to rectify a situation.*
- *Hacktivist. There are several hacking communities that band together for a common cause. Anarchists, racists, animal rights, and environmental protection groups are examples.*
- *Vigilantism. One aspect of hacking that you do not see on the news and in the daily paper is the vigilante groups that surreptitiously attack the Internet’s lower lifeforms, to use their terms.*

3. ÜBER HACKER

- In German, *über* can be loosely translated to “super.” The resulting definition is easy to interpret: “Super Hacker.” An über hacker is a person with exceptional skills, fortitude, and a long list of experiences to draw upon for future hacks.

CHAPTER-3

The Framework

PLANNING THE TEST

- As with anything worth doing, proper planning is essential to performing a successful project. Planning provides an opportunity to evaluate existing business demands and processes, how they relate to a new business endeavor, and to make choices on which characteristics are worth doing and those in which you're not willing to accept risk.
- Existing security policies, culture, laws and regulations, best practices, and industry requirements will drive many of the inputs needed to make decisions on the scope and scale of a test.
- Planning describes many of the details and their role in formulating a controlled attack. Security policies, program, posture, and ultimately risk all play a part in guiding the outcome of a test.

SOUND OPERATIONS

Logistics of the test will drive how information is shared and to what degree (or depth) each characteristic will be performed to achieve the desired results. Operational features will include determining what the imposed limitations of the tester are and how they are evaluated during the test.

RECONNAISSANCE

- Reconnaissance is the search for freely available information to assist in the attack. The search can be quick ping sweeps to see what IP addresses on a network will respond, scouring newsgroups on the Internet in search of misguided employees divulging useful information, or rummaging through the trash to find receipts for telecommunication services.
- Reconnaissance can include theft, lying to people, tapping phones and networks, impersonations, or even leveraging falsified friendships to collect data about a target.

ENUMERATION

- Enumeration (also known as network or vulnerability discovery) is essentially obtaining readily available (and sometimes provided) information directly from the target's systems, applications, and networks. An interesting point to make very early is that the enumeration phase represents a point within the project where the line between a passive attack and an active attack begins to blur. Without setting the appropriate expectations, this phase can have results ranging from "Oops" to "Do you swear to tell the truth and nothing but the truth?"
- The simplest explanation of a port scan is the manipulation of the basic communication setup between two networked systems using TCP/IP as a communication protocol. TCP/IP uses a basic session setup that can be used to determine what application ports a system is willing to use to establish communications.

- the TCP protocol has what is commonly known as the “three-way handshake” that is used to start TCP connections:
 1. Computer A sends a message called a “SYN” (Synchronize) to Computer B.
 2. Computer B acknowledges that message with a “SYN+ACK” (SYN with an Acknowledgement) to Computer A.
 3. Computer A sends back an acknowledgement—“ACK.”

Obviously, collecting information about systems is the first step in formulating an attack plan.

VULNERABILITY ANALYSIS

- The vulnerability analysis phase is a practical process of comparing the collected information with known vulnerabilities.
- Most information can be collected from the Internet or other sources, such as newsgroups or mailing lists, which can be used to compare information about the target to seek options for exploitation.
- However, information provided by vendors and even data collected from the target can be used to formulate a successful attack.
- Information collected during the reconnaissance phase from the company can provide information about vulnerabilities unique to its environment. Data obtained directly from the company can actually support the discovery of vulnerabilities that cannot be located anywhere else.

EXPLOITATION

Exploiting systems and applications can be easy, such as running a tool, or intricate, with fine-tuned steps executed in a specific way to get in. No matter the level of difficulty, good testers follow a pattern during the exploitation phase of a test.

Each test is evaluated at every point within the operation to ensure the expected outcome is met. Each divergence from the plan is appraised to make two fundamental determinations:

1. *Expectations.* Are the expectations of the thread or group not being met or are the test’s results conflicting with the company’s assumptions? The objective is to ensure each test is within the bounds of what was established and agreed upon.
2. *Technical.* Is a system reacting in an unexpected manner, which is having an impact on the test and the engagement as a whole? Much more granular in theory than general expectations of the test, technical gaps are literally the response of a system during the test.

FINAL ANALYSIS

- The final analysis phase provides a link between the exploitation phase and the creation of the deliverable.
- The first goal of the analysis is to take a comprehensive view of the entire engagement and look for other opportunities that may exist, but are not directly observed.

- The final analysis is part interpretation and part empirical results. To define something as critical with little evidence can become problematic when presented to the recipient of the test. However, if there is enough evidence from other threads and groups that prove the vulnerability could represent a substantial risk, it becomes much more palatable and easier to communicate in terms of value and remediation.

DELIVERABLE

- Throughout the history of penetration testing there have been deliverables communicating the results of the test in numerous ways. Some are short, only listing the identified vulnerabilities and where to find the patch to fix them. Others are cookie-cutter reports from tools that simply state which port was open, the vulnerability it represents, and where to find the patch.
- Are these examples of poor deliverables? In reality, no. These are simply the results of a technical test performed in conjunction with the demands of the company.
- Reports from many companies and individuals that are, in a word, exceptional. They provide insightful commentary, step-by-step details, and rank the vulnerabilities to the best of their knowledge and understanding of the customer's business. They provide measurable levels of risk, raw results from the test, where backdoors are, how they were placed, and how to remove them.
- It is my expectation that the recipients of deliverables—good and bad—would like to know what a good deliverable should include and ultimately how to translate it into valuable security improvements.

INTEGRATION

- how to use the test to your full advantage is directly dependent on the proposed integration process.

There are three distinguishing factors that should be considered during the integration of any test results:

1. *Mitigation.* If something were found that represented a threat to secure operations and was beyond acceptable risk, then it would need to be fixed, to put it bluntly.
2. *Defense.* Defense planning is establishing a foundation of security to grow on and ensure long-term success.
3. *Incident Management.* Arguably, the core element of security—the ability to detect, respond, and recover from an attack—is an essential part of any security program. Knowing how you were attacked, the vulnerabilities exploited, and the potential impacts aids in formulating an incident response plan.

CHAPTER-5

Information Security Program

THE PROCESS OF INFORMATION SECURITY

- Effective information security is an iterative process. The process must identify and mitigate present risk, as well as allow feedback into the process to mitigate future risk.
- When developing an information security program, the instinctive first step is to look at the technical and managerial structure of an organization in an effort to determine the best course of action based on the industry's security demands communicated by best practices, standards, and regulations.
- However, by beginning at a much higher level, risk, the program will be aligned to business elements and not be influenced by the nuances of technical firefights and dissimilar management practices.
- By approaching the creation of a security program by using the element of risk, the process is much more efficient and applicable in the end.

COMPONENT PARTS OF INFORMATION SECURITY PROGRAMS

RISK ASSESSMENT

- The risk assessment process requires creation of an initial security domain definition to set the scope of the assessment by acknowledging the span of control and relevant assets.
- This corresponds to the security architecture model (extended, perimeter, control, and resource layers) by defining physical and logical boundaries and tabulating assets at risk.

MANAGEMENT SYSTEM

The information security management system functions to address risk, whether it is accepted, transferred, or mitigated; information security management systems are beginning to enjoy the adoption of internationally recognized standards, and are increasingly being seen as analogous to Total Quality Management (TQM) systems, managing the quality of information security.

One rapidly emerging internationally recognized standard is ISO17799, heir apparent to the venerable BS7799 standard, and focused on ten functional control areas including:

- *Information Security Policy* addressing management support, ongoing commitment, and direction in accomplishing information security goals;
- *Organizational Security* addressing the need for a management framework to create, sustain, and manage the security infrastructure;
- *Asset Classification and Control* addressing the ability of the security infrastructure to protect organizational assets;
- *Personnel Security* addressing an organization's ability to mitigate risk inherent in human interaction;

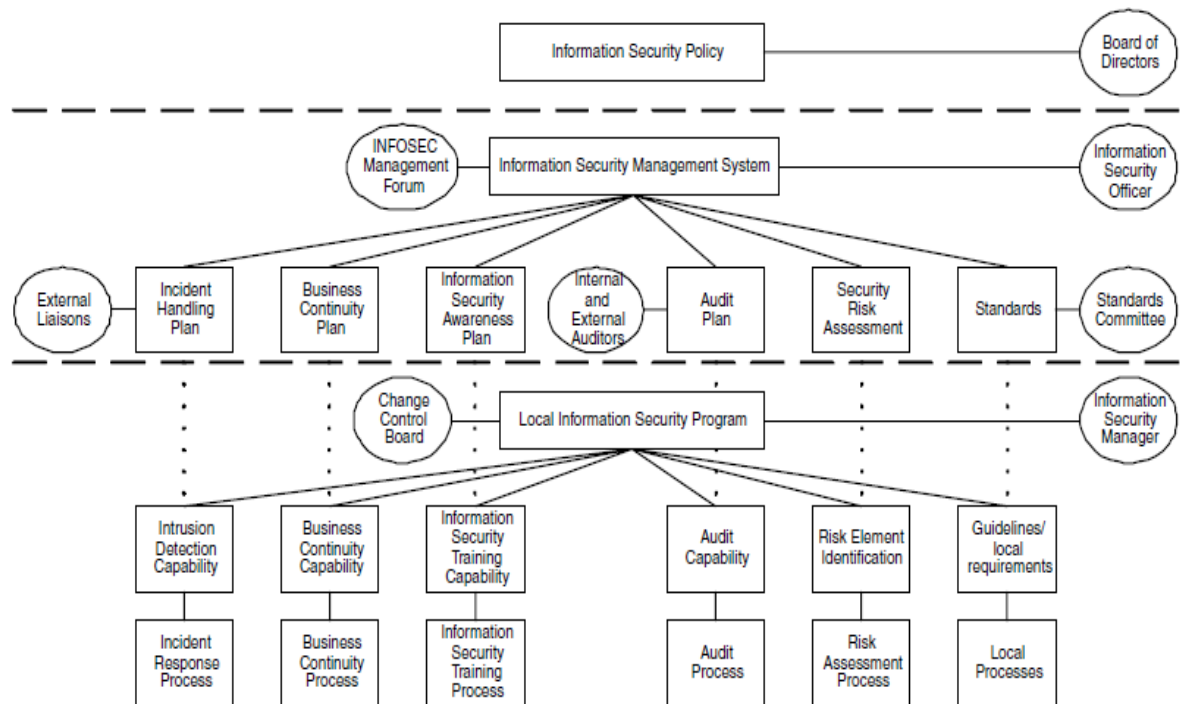


FIGURE 5.4 Example of an Information Security Program Structure

- *Physical and Environmental Security* addressing risk inherent to the organization's premise;
- *Communications and Operations Management* addressing an organization's ability to ensure correct, secure, and repeatable operation of its assets;
- *Access Control* addressing an organization's ability to control access to assets based upon business and security requirements;
- *System Development and Maintenance* addressing an organization's ability to ensure that information system security controls are both incorporated and maintained;
- *Business Continuity Management* addressing an organization's ability to counteract interruptions to normal operations; and
- *Compliance* addressing an organization's ability to remain compliant with regulatory, statutory, contractual, and security requirements.

Security management based upon ISO17799 takes a very holistic look at information security and at all aspects of an organization's ability to manage risk.

Security organizations address the individual's role in the security program.

- *Functional Roles* allow assignment of specific security responsibilities such as Information Security Officers.
- *Information Security Management Committees* are chartered with specific tasks such as Configuration Control Boards.
- *Multidisciplinary Management Forums* are tasked with promoting information security awareness throughout the organization with codified practices that refine an organization's risk mitigation strategy to a level of granularity that can be implemented.
- *Policies* express conceptual goals of upper management defining the risk mitigation strategy.
- *Standards* define measurable requirements in support of policy goals.
- *Guidelines* offer best practice advice on how to meet standard requirements.

- *Procedures furnish step-by-step instructions to create a consistent and repeatable process.*

Ancillary programs address risk not addressed by security organizations or codified practices. In some organizations, these ancillary programs may liaise with the security program, but be externally managed. For example, business continuity may stand alone, or security awareness may fall under HR or training.

- *Business Continuity programs ensure the sustainability of the organization.*
- *Incident Management programs respond to anomalies.*
- *Security Awareness programs educate an organization's personnel on information security issues.*

RISK ANALYSIS AND ETHICAL HACKING

- One of the predominant questions fielded during discussions about security, and especially about ethical hacking, is the delineation between a risk analysis and an ethical hack.
- Much of the decision to employ a risk analysis over an ethical hack, or vice versa, is based on interpretation, scale, goals, and cost. The immediate assumption is that a risk analysis would take more time, consume more resources, and cost significantly more than an ethical hack.

TABLE 5.1

Role of Ethical Hacking and Risk Analysis in Evaluating Security

Evaluating Threats and Vulnerabilities	Determining Effectiveness of Security Controls	Establishing Value of Assets
Ethical hacking	Ethical hacking and risk analysis	Risk analysis

TABLE 5.2

Pros and Cons of Ethical Hacking and Risk Analysis

Scenario:	Assessing Security of Internet-Facing Infrastructure	
Ethical Hacking (Typically Employed)	Pros: Identifies technical vulnerabilities Determines exposure to threats Establishes the level of effort required to exploit a vulnerability Provides a perspective of the infrastructure from an unknown entity (i.e., Internet public, competitor, etc.) Technically comprehensive (scan entire networks and groups) Provides information on necessary tools and tactics required to attack firewalls, services (e.g., DNS, FTP, etc.), and other infrastructure elements	Cons: Does not consider management practices and security policy Potentially affected by firewall or other chokepoint capabilities Exposure to detection by IDS/IPS or other monitoring Potential for adverse events (e.g., downtime, damage, etc.) Does not provide information or recommendations regarding elements outside of immediate observation Does not take asset value into consideration (Note: this is performed only through the tester's perception, not documented asset classification)
Risk Analysis	Pros: Considers all aspects of information security: technical configurations, management, operations, and policy (among others) Does not present a risk to the operations of Internet applications and systems Comprehensive configuration analysis of routers, firewalls, and systems Provides a detailed analysis of risk to Internet-facing systems, networks, and applications based on traditional Internet threats	Cons: Vulnerabilities are determined through investigation, not empirical evidence from system interaction Assumes level of effort to exploit a vulnerability Assumes potential vectors of attack (i.e., does not test for alternate routes to assets, but assumes them based on infrastructure Performed based on sampling or light vulnerability scanning (potentially not comprehensive)
Results	Ethical Hacking: Itemized list of vulnerabilities found on the Internet-facing systems An understanding of depth attained from the Internet Detailed analysis of exploitation, tools, and tactics used against the identifiable systems Raw data from the test Recommendations for remediation	Risk Analysis: Detailed analysis of security policies and practices used to manage the security controls Analysis of security architecture and recommendations for modification Asset valuation and exposure to common Internet threats Recommendations for remediation

Scenario:	Assessing Security of Specific Custom Web Application	
Ethical Hacking (Typically Employed)	Pros: Directly tests user data input and potential for processing errors Evaluates any client-side scripting, applications, or plug-ins Tests potential performance issues Can expose technical weaknesses permitting access to private information Manipulates cookies or other programming attributes to exploit the application	Cons: Does not include (typically) access to code or application elements not published or provided Does not address the planned applications developments Is not aware and cannot clearly evaluate the infrastructure attributes Does not address the management, operations, or processes supporting the application
Risk Analysis	Pros: Evaluates the supporting infrastructure and can make security recommendations on information flow controls Access to supporting data, systems, and business data to specifically determine level of impact Evaluates authentication procedures and interaction with supporting elements Can clearly determine the impact to the organization in the event of an outage or breach of security Identifies errors and opportunities for improving application development processes	Cons: Vulnerabilities in the application are based on code, process, and previous development phases and not on technical observation May not address client-side technical elements and make assumptions on remote system vulnerabilities Does not look for other, unrelated technical avenues for attack Cannot clearly evaluate the options to threats given various forms of attack
Results	Ethical Hacking: Detailed list of vulnerabilities and the level of access attained from exploitation Comprehensive understanding of software flaws and the resulting immediate impact	Risk Analysis: Detailed analysis of the potential impact in the event of attack Evaluation of software development practices Security review of the code

TABLE 5.3
Pros and Cons of Ethical Hacking and Risk Analysis (continued)

Scenario:	Assess Level of Risk from Internal Employees	
Ethical Hacking	Pros: Perform social engineering from outside or as an employee to evaluate the level of access and impact of an internal resource Can use vulnerability scanning tools to seek opportunities for greater access Directly exploit vulnerabilities (i.e., access secured areas, collect materials from other employee's desks, system access, etc.)	Cons: Potentially time consuming Limited to approved social engineering testing options Limited to the experience and capability of the tester Not exposed to defined policies, roles and responsibilities, and management processes Exposed to discovery
Risk Analysis (Typically Employed)	Pros: Evaluates the entire infrastructure for potential physical, network, and system (application) access Can evaluate the level of security controls based on business requirements Evaluates the existence of various level of controls and implementation Exposed to the interdependencies related to systems, departments, geography, and partnerships	Cons: Does not clearly evaluate the access of a given employee Must address all elements of the internal environment, even if a focused effort Does not test specific applications or technical solutions to determine discrete access
Results	Ethical Hacking: A detailed analysis of potential problems from one or a small group of employees Provide technical insights to internal network and application vulnerabilities Can provide specific materials and access available to internal employees and communicate the results	Risk Analysis: Detailed analysis of potential threats based on internal controls and configuration Analysis of employee management practices Evaluation of internal controls, policies and procedures, and recommendations

Scenario:	Assess Security of Internal Network or Segment	
Ethical Hacking (Typically Employed)	Pros: Provides greater insight to the scope of opportunities to internal employees to interact with systems and other networks Identifies discrete vulnerabilities at all layers in the network (i.e., physical, IP, services, systems, and applications)	Cons: Due to the openness of the infrastructure, it significantly increases the potential for affecting business operations Can result in an inordinate amount of vulnerabilities to sift through to determine next steps Assumes internal threats are sophisticated
Risk Analysis	Pros: Evaluates the infrastructure through controlled observations rather than explicit testing Not limited to the immediate technical environment and conclusion can be determined based on business-level information Information about vulnerabilities is typically associated with architecture and process (i.e., configuration management, access controls) as opposed to specific vulnerabilities	Cons: Does not clearly represent the perspective from an internal system on the network, or someone with specific credentials Does not typically provide specific vulnerabilities about systems or applications based on direct interaction
Results	Ethical Hacking: A list of vulnerabilities and how they were identified and potentially exploited Assists in fixing technical issues	Risk Analysis: Detailed analysis of the internal architecture and the potential exposures based on observations Assists in addressing the high-level technical concerns in addition to process changes

TABLE 5.4
Pros and Cons of Ethical Hacking and Risk Analysis (continued)

Scenario:	Assess Physical Security	
Ethical Hacking	Pros: Evaluates the security controls inherently designed to thwart human threats (See Note, Ch. 9: "The Physicality of Social Engineering") Has the potential to accurately reflect various threats Provides the option of comprehensive control and granularity	Cons: Requires substantial planning to ensure the potential threat is replicated Increases the liability associated with exploitation of physical controls
Risk Analysis (Typically Employed)	Pros: Determines the level of threat and vulnerabilities through evaluation of security controls Assesses the policies and procedures related to physical controls	Cons: Does not assess security based on tested weaknesses Level of threats and vulnerabilities based on interpretation of the controls as opposed to testing
Results	Ethical Hacking: Provides a list of vulnerabilities that contributed to the failure of controls Offers a detailed understanding of what is obtainable to a person at various points or stages in the test A detailed explanation of what was performed to thwart the security controls	Risk Analysis: Detailed analysis of physical controls, potential vulnerabilities, a collection of threats, and likelihood of exploitation Provides a collection of broad recommendations, including policy and process, to accommodate potential weakness