

Unit I

Introduction

* Hacking is computer crime that can result in massive financial losses for companies, governments, and individuals.
* The costs associated with computer crime can range from 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.
* Resources.
* Resources are computer-related services that perform actions or tasks on the user’s behalf.
* Core services, object code, or disk space can be considered resources that, if controlled, utilized, or disabled by an unauthorized entity, could result in the inability to capture revenue for a company or failure to meet expected objectives.
* Information.
* Information can represent an enormous cost if destroyed or altered without authorization.
* Data can be affected in several ways such as: loss, disclosure, and integrity.
* 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.
* Anything that consumes time, consumes money, and expenditures for recovering from an incident can represent the greatest form of financial loss.
* Brand and Reputation.
* There are many companies who have very recognizable brands, like color alone will promote images.

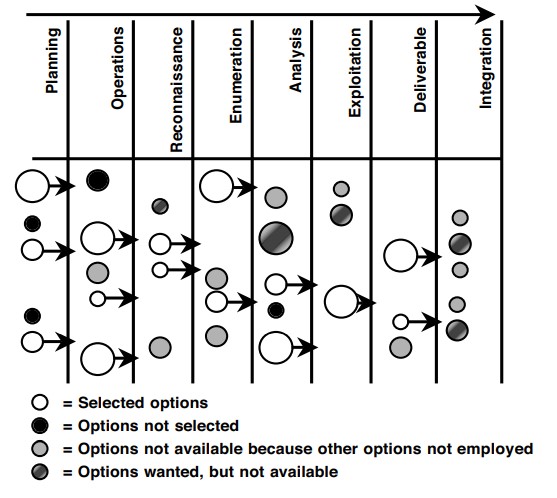
# The Hacker

* First of all, the term “hacker,” historically speaking, is inaccurate. 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

* Here 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
* Script kiddies
* “Script kiddie” refers to a hacker who influences tools created by other, more knowledgeable hackers to perform malicious acts.
* There are several degrees of damage that can be caused by people who fall into this category.
* Script kiddies can be grouped into three areas: unstructured, structured, and determined.
* Hackers
* Hackers are the next step in the evolution of an attacker and make up the majority of the people.
* Hackers explore computers for education, the challenge, and to achieve a social status among other hackers.
* There are four distinguishing faculties of the hacker: malicious, solvers, hacktivist, and vigilante.
* 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.
* 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.
* 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.
* 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.
* These are the elite and nearly unstoppable hackers.
* To be an über hacker you must have exceptional skills in programming, logic, systems, operating systems, applications, hardware, communications, and protocols along with a strong dose of attitude and unethical behavior.

# Framework



# Planning the 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.
* What drives a company’s focus on security, its core business needs, challenges, and expectations will set the stage for the entire engagement.

# Sound Operations

* How is the test going to be supported and controlled?
* What are the underlying actions that must be performed regardless of the scope of the test?
* Who does what, when, where, how long, who is out of bounds, and what is in bounds of a test all need to be addressed.
* 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.
* 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.
* TCP/IP uses a basic session setup.
* More technically, 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.”

# Vulnerability Analysis

* There is a logical and pragmatic approach to analyzing data.
* During the enumeration phase, we try to perform an interpretation of the information collected looking for relationships that may lead to exposures that can be exploited.
* The vulnerability analysis phase is a practical process of comparing the collected information with known vulnerabilities.

# Exploitation

* A great deal of planning and evaluation is being performed during the earlier phases to ensure a business-centric foundation of value is established for the test.
* The attack process is broken up into threads and groups and each appears in sets of security.
* A thread is a collection of tasks that must be performed in a specific order to achieve a goal.
* Threads can be one step or many in a series used to gain access.
* Each divergence from the plan is appraised to make two fundamental determinations:

# Exploitation-

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.
   * Keeping your eyes open for unexpected responses from systems ensures you have not negatively affected the target or gone beyond the set scope of the test.

# Final Analysis

* Although the attack process has many checks and validations to ensure the overall success of the engagement, a final analysis of all the collected data and exploits must be performed.
* 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

# 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.
* There are some that detail every move made by the consultant: Cracked the passwords, and took over your shipping application and of course where to find the patch.

# Deliverable-

* Are these examples of poor deliverables? In reality, no.
* In addition, ethical hacking has become so common that if a deliverable doesn’t drive fear into the hearts of the executives it could be considered a failure.

# Integration

* The deliverable communicates all the necessary information needed to actually support some form of integration.
* The deliverable can be combined with existing materials, such as a risk analysis, security policy, previous test results, and information associated with a security program to enhance mitigation.
* There are three distinguishing factors that should be considered during the integration of any test results:
  1. Mitigation.
  2. Defense
  3. Incident Management.

# Integration –

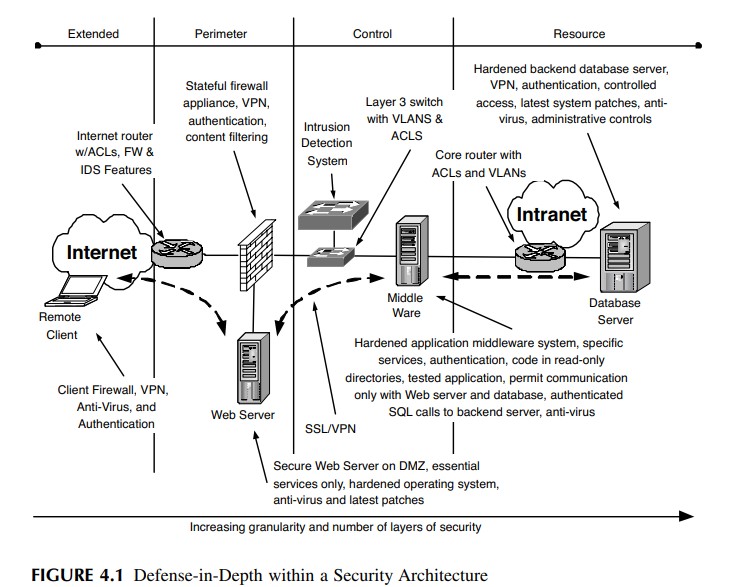
* Mitigation.
* If something were found that represented a threat to secure operations and was beyond acceptable risk, then it would need to be fixed, to put it bluntly.
* Of course, there are the easy things to rectify and there are very complicated solutions to seemingly simple problems.
* Mitigation of a vulnerability can include testing, piloting, implementing, and validating changes to systems
* Defense.
* How should you address the insecurities in a strategic manner?
* What about your networks, systems, applications, and policies that need to be addressed to ensure sound practices are employed to minimize the impact of future or undetected vulnerabilities?
* Defense planning is establishing a foundation of security to grow on and ensure longterm success.

# Integration –

* 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.
* The test provides an opportunity for you to learn about the various weaknesses and attractive avenues of attack.
* Finally, you get an understanding of critical points in the network that may need more attention than others, and this may not be the perimeter as normally assumed.

# Information Security Models

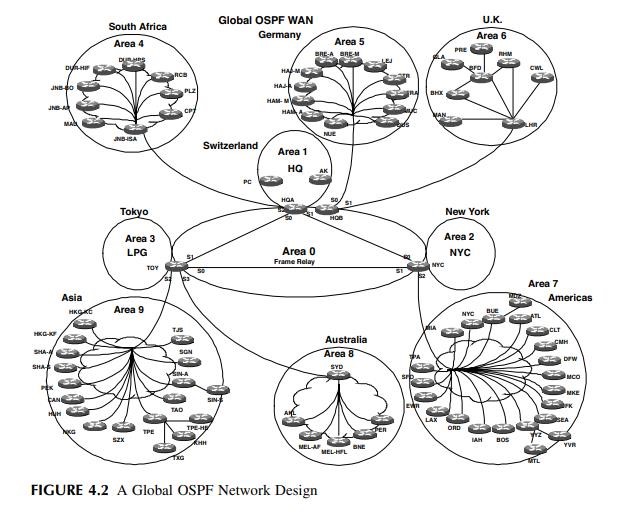
* Information security has heard the term “defense-in-depth,” the practice of building many layers of security into systems, networks, Security and applications.
* Defense-in-depth is creating several controls that are unique, but complement each other to provide effective protection.
* The defense-in-depth model is defined in four layers:
  1. Computer security
  2. Network security
  3. Service security
  4. Application security
* These models are combined and demonstrated in the following figure.

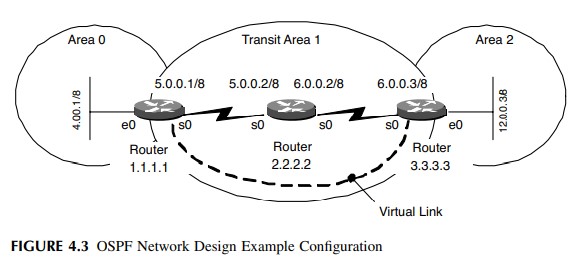


* Computer Security
* Computer security includes many diverse subjects, such as controlling authorized (and unauthorized) access, managing user accounts and their privileges, software management, change control, development, and database security, to mention a few.
* Much of the security is afforded by the operating system responsible for providing the interface between the hardware and the software and ultimately the user.
* Operating systems come in many types and flavors.
* Microsoft’s Windows is the most prevalent operating system used today for home and business.
* UNIX, an operating system born in Bell Labs, has many flavors and versions, such as Linux, BSD, Solaris, and AIX, to name a few of the popular ones.
* Computer security, better yet the lack of, could be considered the flashpoint for the birth of the common hacker.
* The pains we’re experiencing today, the constant focus on the perimeter as the primary security provider, the explosion of viruses and worms, and the constant battle of integrity and reliability, all stem from the poor evolution of computer security.
* Operating system security will not solve world hunger, but a secure system allows greater investment in access controls, comprehensive network security, and application security with less focus on viruses and small holes that lead to big results.
* HARDEN A SYSTEM Determining what steps are necessary to harden a system can be very frustrating.
* There are numerous sources of various tactics for securing a system. There are sample configurations and tools that can be used to configure Microsoft and UNIX systems.
* The following are some common characteristics of hardening a system.
* Physically Secure It
* Installing the Operating System
* Get It Running
* Get It Running
* Cleanup
* There are three types of patches:
  + 1. Functionality. A patch that fixes or enhances a certain function of the system. For example, how memory is handled, performance of network connections, or adding more options to an administrative program.
    2. Feature. A feature patch increases the use of the system, an added feature.
    3. Security. A security patch fixes a vulnerability in the system due to unexpected conditions the system is in or a misstep in programming.

# Information Security Models –

* Network Security
* Networks are relatively simple.
* When a computer wishes to establish communications with another it generates a message augmented with a header, containing logistical information about the source and destination, and the entire package is called a packet.
* As with computer security, there are various characteristics of network security. These are summarized in the following list:
* Transmission Security: The protection of data as it is transmitted from one location to another.
* Protocol Security: The construction of packets and how they are processed and used to transmit information.
* Routing Protocol Security: The information that is shared by network devices to work together to support communications.
* Network Access Security: Controlling connectivity from one network to another based on protocol specifics.
* TRANSMISSION SECURITY
* One aspect of network security is the protection of information in transit.
* Ensuring sensitive data is protected from unauthorized changes or viewed by unauthorized people (or applications) is an important aspect of secure network communications.
* Security protocols, such as IPSec (Internet Protocol Security), SSL (Secure Sockets Layer), and SSH (Secure Shell) to name a few, provide authentication and encryption to protect information from unwanted interactions.
* There are also protocols that usually work in cleartext.
* File Transfer Protocol (FTP) and Telnet are interactive sessions between systems that are not provided any protection to keep the commands and passwords private.
* PROTOCOL SECURITY
* Another characteristic of network security is the protocols that are used to support the communication.
* Transmission Control Protocol and Internet Protocol (TCP/IP) is the most common protocol used today and is the protocol for use on the Internet.
* A protocol is the standard by which a communication is established.
* There are many protocol weaknesses that are associated with TCP/IP.
* By using illegal packet structures and manipulating the session management the protocol provides, several types of attacks can materialize.
* Other weaknesses in the protocol allowed one system to appear as another.
* This was an especially effective attack when security was based on assumed trust relationships based on an IP address, the unique identifier of a system on a TCP/IP network.
* Second, because the hacker is not receiving the acknowledgments, he must respond in the appropriate timeframe with all the correct information expected by a normal session.
* ROUTING PROTOCOL SECURITY
* Routing protocols are specific communications between network supporting systems that allow the sharing of network information so a group of devices can collaborate on appropriately forwarding data.
* When routing data is shared among a group of systems communications can be routed based on network availability, performance, and cost of the connection.
* Figure (next slide) is an example of a large network supported by the OSPF (Open Shortest Path First) routing protocol. OSPF uses “areas” to define borders for summarizing network routes to different regions, as with this example, or departments.



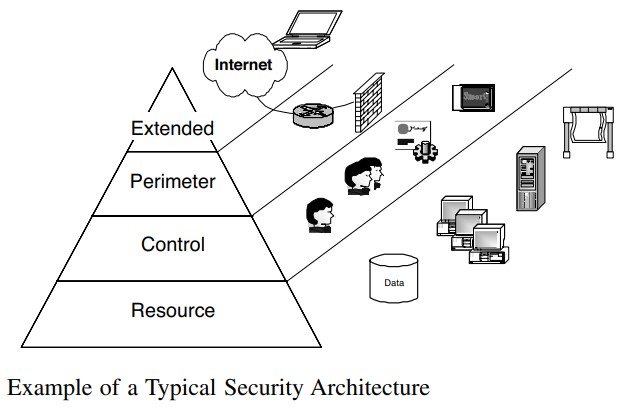


* NETWORK ACCESS CONTROLS
* Network security can also be characterized by applying access controls, limiting the availability of communications between systems or applications.
* In TCP/IP headers there are collections of bits that identify specifics about the communication.
* Application ports are an example of this type of information.
* The port is a number from 1 to 65535 that identifies the services associated with the communication.
* Application ports allow systems to accept packets destined for specific services or applications.

# Information Security Models –

* Service Security
* Services are processes that run on a computer to provide common functions for applications, users, or other services. Services fall into two very similar categories:
  1. Operational. A process that provides a service to applications or users for functionality.
  2. Network. A process that supports the exchange of information for network services.
* The following are examples of operational services used in Microsoft Windows:
* Security Accounts Manager. Stores security information for local user accounts.
* Plug and Play. Enables a computer to recognize and adapt to hardware changes with little or no user input.
* Net Logon. Supports pass-through authentication of account logon events for computers in a domain.
* Event Log. Enables event log messages issued by Windows-based programs and components to be viewed in Event Viewer. This service cannot be stopped.
* Regardless of type, each service is an opportunity to attack a system.
* Potential vulnerabilities in how services interact with a network, applications, and other parts of the operating system make them the focus of hackers.
* Application security
* As we climb up the layers of security, applications represent the last step.
* An application, especially software, is a collection of libraries, executables, and other utilities used to accomplish a wide variety of tasks.
* Applications can come with their own forms of vulnerabilities and weaknesses that could be used by a hacker.
* Some of these are benign from the perspective of the Internet because they require complete access to the system.
* Software introduces its own set of security concerns.
* Applications can have errors, better known as bugs, which can not only disrupt operations but can provide a hole through which a hacker can crawl.
* A software error can lead to massive failures such as implementing a rare configuration that exposes a bug in the software.
* There are ample examples of these types of vulnerabilities that can be used by a hacker in many ways. Following are a few examples:
* Exchange Server 2000 System Attendant gives the “Everyone” group privileges to the WinReg key, which could allow remote attackers to read or modify registry keys.
* • Internet Explorer 5.01, 5.5, and 6.0 allow remote attackers to read files on a remote system via malformed requests to the GetObject function, which bypasses some of GetObject’s security checks.
* When executed correctly, code reviews will uncover many straightforward but dangerous security violations, such as:
* Buffer overflows
* Race conditions
* Tainted input
* Format string issues
* Trust management
* Third-party package connectivity
* Input validation
* Temporary file or memory usage
* Poor cryptography
* Appropriate logging and auditing

# Security Architecture



# Security Architecture

• Commonalities among many of the architectures that are available are four layers that can be identified to promote sound security integration and management of technology, information, and policy:

1. The resource layer is where services and data reside. It is the home of servers, applications, databases, workstations, and storage.
2. One of the more critical and complex is the control layer, which provides identity and access management services. Moreover, the control layer is the point where policy becomes reality in the technical space. It provides management with the policy and is the point where policy is bound to data to promote greater authorization across the other characteristics of the entire security architecture.
3. There is the perimeter layer, which enforces a logical boundary between the Internet and the intranet, departments, applications, and even users.
4. Finally, the extended layer is a growing entity in its own right. This represents the externally facing envelope of influence and security, such as remote access risks, application access, and E-commercelity in the technical space. It provides

# RESOURCE LAYER

* Resources, as previously defined, are systems, applications, internal users, databases, services, printers, local area networks, operating systems, and data.
* Resources represent what organizations feel are their core technical requirements to make money, or supporting mechanisms for the evolution of the business as a whole.
* Nevertheless, resources are effectively what you want to protect, control access to, and use to conduct business.
* In that light, not every resource demands the same level of security. It is not uncommon to have useful information destroyed with little or no impact on the business operations.
* On the other hand, the slightest unauthorized change or loss of a specific piece of information can be catastrophic.

# CONTROL LAYER

* The control layer is an opportunity to identify and group systems that manage access to resources.
* In a perfect world all identification, authentication, and authorization to resources would be controlled by a single system.
* Thanks to legacy systems, different application architectures, and different approaches to applying security controls, the control layer is typically made up of many diverse products.

# PERIMETER

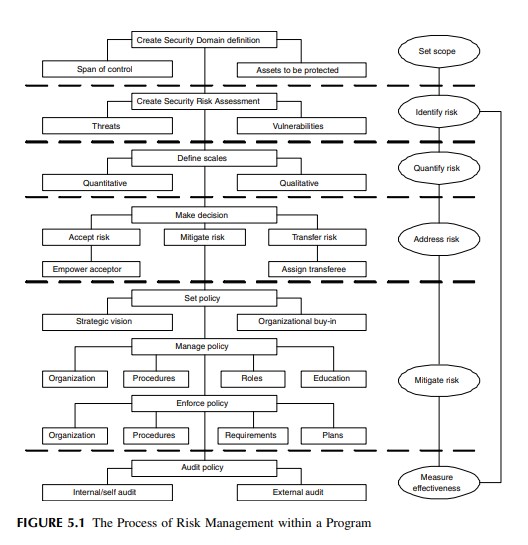
* Perimeter security is the most obvious layer in the security model.
* Basically, it’s where your network stops and someone else’s begins.
* It can be your connection to the Internet, the segregation of certain system types, or business units with different security needs.
* Suffice it to say, the perimeter is usually easily identifiable.
* The perimeter is much more than a firewall and there are other technologies that promote secure communications between trusted and not-so-trusted networks.
* Intrusion detection and, most recently, intrusion prevention systems have provided another layer of security for the perimeter.

# EXTENDED

* The extended layer is how corporate security is projected out into the ether.
* The most basic example is customers going to Web sites that have a security policy defining how information collected from online transactions is used.
* Roaming users are another example of how corporate security influences information protection beyond the perimeter.
* Organizations are concerned with the security of their intellectual property, brand name, and various information assets that are accessed and shared in many ways with varying types of users.

# Information Security Program

* A security program is concerned with preserving the confidentiality, integrity, and availability of an organization’s information assets and information should be considered an asset in whatever form.
* This is a “big picture” approach to enhance the breadth of risk analysis, requiring a multidisciplinary look at risk identification.
* Ethical hacking is testing security through the act of exploitation, the exploitation of anything that is assumed to provide a layer of control protecting resources, information, or other forms of assets.
* A security program defines the necessary characteristics to ensure each layer of security is working in accordance with expectations, in addition to ensuring continuity of security from one layer to another

The Process of Information Security

# Component Parts of Information Security Program

* RISK ASSESSMENT
* MANAGEMENT SYSTEM
* CONTROLS
* MAINTENANCE PLAN

# Program –

* RISK ASSESSMENT
* An information security risk assessment identifies and quantifies risk, thus serving as the basis for addressing risk.
* 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 by defining physical and logical boundaries and tabulating assets at risk.
* MANAGEMENT SYSTEM
* 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.

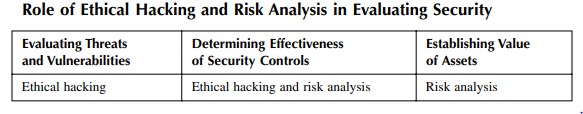
CONTROLS

* Controls come in many forms, including physical devices, configurations, roles, and processes, affecting networks, platforms, roles, and operations.
* Many controls require subordinate or supporting controls. For example:
* A firewall is a network control device used to enforce network access and service requirements.
* The firewall requires: – A supporting procedure for authorized users and services – A supporting role to administer the device – A supporting organization for configuration control

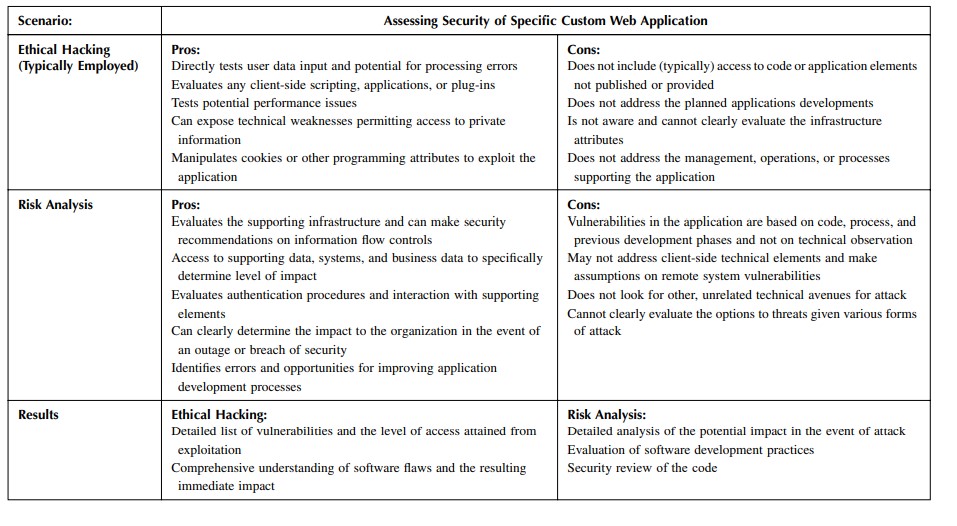
MAINTENANCE PLAN

* An effective security program must always be considered an ongoing initiative, subject to regular maintenance.
* Controls deployed today will only meet the current threat environment, and tomorrow is another day.
* The program maintenance plan validates protection of the security architecture model, addressing both security program review and audit.
* Program review should start at the top with yearly reaffirmation of program goals by upper management.

Risk Analysis and Ethical Hacking.



# Risk Analysis and Ethical Hacking-



Unit II

# The Business Perspective: Business Objectives

* So what is the objective of the test?
* Why are you considering permitting someone to hack your network?
* What do you expect to learn and are you prepared for the results?
* Do you have the capabilities to address the identified issues? The answer to these questions is:

Take security seriously and people who perform ethical hacks will tell you that even the most robust firms fall quickly.

But, is this a reflection of poor security practices, or poor planning of the test? There are many characteristics of security and how security is realized in a company.

The number of people responsible for security, their practices, and job pressures will have an impact on how the perception of security is materialized in the systems and applications.

# Security Policy

* At the most fundamental level, a security policy is comprised of collections of statements, with each containing supporting material.
* A policy statement generally defines the organization’s stance on a particular aspect of information security.
* The supporting material behind a policy statement consists of standards, guidelines, and procedures that outline specific processes to enforce the policy.
* Policy Statement. Policy statements should be clear statements on the particular aspect of security that provide no room for interpretation. They should provide generalized, yet pertinent information on what is expected to be practiced within the organization.
* Policy statements should avoid justification of the policy, details that are supported by the standards, guidelines, or procedures, or any specific technology associated with the policy. All these characteristics tend to add complexity and open the opportunity to interpretation. Allow the details to be addressed in the supporting statements.
* Standard. A standard is the actual definition of the technical nature of the requirement communicated by the policy statement. Standards provide specific details that explain or quantify the policy statement with which they are associated. Standards should be detailed and clear in communicating the requirements of the policy statement by quantifying the necessary attributes of the policy. However, the standard should not include procedures or step-bystep processes on how to implement the policy. The goal is to define the final structure associated with the statement.
* Guideline. A guideline is a collection of supporting activities to help associate everyday activities with the support of the policy statement. Guidelines provide general suggestions or recommendations that further clarify the policy with general details or suggestions for their implementation. Without guidelines, the policy statement and standard would have little meaningful impact on the typical user. To accomplish this, guidelines should provide associated technologies and guidance in various conditions. However, once again, the processes for carrying out the policy should not be addressed within the guidelines.
* Procedure. A procedure defines the tasks required to meet the requirements set forth in the policy. Procedures are step-by-step instructions detailing how a particular task is to be performed. These are executed to implement and enforce policy statements, or to measure the organization’s compliance with a particular statement for later auditing purposes. Procedures should be very clear on performance of necessary tasks and should avoid any information outside the scope of simply providing the steps to complete and enforce

# Previous Test Results

* There are many organizations that have tests performed regularly with their own set of results, recommendations, and implemented countermeasures.
* The deliverables from a previous test provide the opportunity to plan a new ethical hack in a manner that is complementary to previous investments.
* For example, a company may have identified specific vulnerabilities during the previous test resulting in the acceptance of that risk.
* To continue testing a risk that has been identified and absorbed into the client’s acknowledged exposure can be a waste of time.
* Nevertheless, vulnerabilities change with the ebb and flow of technology. Therefore, assumptions about identified weaknesses should not be made lightly. Finally, and much more common, is that the testing firm can review the previous test results to test the identified vulnerabilities the customer has assumed have been fixed since the last test.
* Although this has more of an audit flavor, the services firm can move on to other areas after verifying that the holes were fixed.

# Business Challenges

* In spite of the risks to achieve business goals companies understand the need to accomplish several fundamentals to ensuring the success for the overall business:
* Meeting financial and business objectives
* Maintaining and increasing corporate brand value and corporate reputation
* Protecting their network infrastructure investment
* Executing and protecting strategic initiatives (mergers, partner alliances, etc.)
* Providing a friendly and secure E-business environment
* Supporting a remote-based employee environment
* Reducing the time to market for providing new services to users and end clients

# Planning for a Controlled Attack: Inherent Limitations

* Inherent limitations are those restrictions that are associated with paying someone to perform an act normally practiced by criminals from a completely different culture and mindset.
* Following are some of the limitations that are intrinsic to the test:
* Time. The time a real hacker is afforded to collect information, gather tools, test the waters, get to know people, or any other aspect of hacking that can be used to obtained what is desired is arguably limited to only that person’s life expectancy.
* Money. It should not be assumed that hackers don’t have any money. In reality, depending on the role they may play in organized crime, substantial investments may be made in providing them all the necessary tools and technology to perform their deed
* Determination. Tenacity can play a significant role in how a hacker approaches a target.
* Legal Restrictions. Regardless of a legal documentation put in place to protect the tester from typical activities that under normal circumstances would be considered illegal, a virtual line remains separating the typical attack strategy from an act of terrorism
* Ethics. In every professional’s career he is at one point faced with a dilemma that forces a decision based solely on his ethics. It’s safe to say that security consultants have ethics in how they work with clients and others in the industry.

# Imposed Limitations

* The ability to realize the true value of a penetration test is proportionate to the client’s interpretation of security and how those assumptions are translated into restrictions placed on the test.
* Limitations can be introduced by the customer for many reasons that can range from financial restrictions, which force less time and inherently reduce the scope of the engagement, to restrictions based simply on political positioning, personal perspectives on security, or a misguided attempt to focus the test.
* Imposed limitations are elements of the test that are not employed for reasons that may not have anything to do with security. I
* n fact, one could argue that imposed limitations have nothing to do with security at all and materialize to simply promote control of the engagement.

# Timing is Everything

* Security is constantly changing within an organization.
* Through the adoption and evolution of technology, practices, management, and the perception of security within the company, the security posture of a firm rises and falls frequently.
* Many characteristics of security increase, decrease, or simply fluctuate with time.
* As one characteristic gets more attention, others are certainly going to wane or grow stagnant
* Security is the combination of technology, management, culture, and policy, and it is difficult to do all of them at the same time in the challenging environment of a typical company.
* Therefore, elements of security begin to suffer and become fragmented due to the lack of attention and ultimately action by the company.
* Where a penetration test is performed, the cycle of security within an organization can affect not only the outcome, but also the value of the test.
* It is not only essential to ensure the test is reflective of the threats the client is concerned about, but the extent of the test, and even if the test should be performed, should be weighed heavily

# Attack Type

* it is possible to reduce their activities into two basic areas that allow us to glean more information about hackers and their targets.
* 1. Opportunistic. An opportunistic attack is the result of hackers looking for vulnerable systems rather than systems with specific information for the taking.
* Usually this is reflected by the plethora of hacks that follow a vulnerability report and the launch of a worm that uses a vulnerability to spread itself and cause trouble.
* In all cases, the target was identified after the vulnerability was discovered and then exploited.
* Typically, these attacks are preceded by a port scan or some form of discovery process that exposes the vulnerability.
* Although this may seem innocuous, many of the hacks on the Internet can be attributed to this type of attack.
* Mostly, the result is a denial of service, Web defacement, or temporary loss of data.
* What can be disturbing is the number of highly effective attacks that are based on using the initial vulnerability as a beachhead to launch a much more devastating attack
* . 2. Targeted. A targeted attack is the assumption that the hacker knows the target and knows what she wants to accomplish.
* Although this is based on whether the attacker is looking for any type of vulnerability to gain access, as opposed to looking for a specific vulnerability for any type of company, an arguably indeterminate metric, it does demonstrate the basic approach of a hacker.
* Therefore, one would rightly conclude that ethical hacking is a targeted attack type.

# Source Point

* There are several types of attack that can be employed to help a company determine its exposure. Typically, these are broken into three major areas, each resulting in various conclusions about where the attack is launched.
* 1. Internet. When you hear the term ethical hacking you immediately picture someone hacking into a network from the Internet.
* In most cases, this is a reality.
* The Internet is seen as the source for all the pains associated with hackers, even though statistics tell us that equal loss is attributed to internal threats.
* Nevertheless, in most penetration-testing engagements, the Internet is the source point of the attack.
* This helps an organization determine its exposure to the plethora of attacks represented by an endless sea of threats.

2. Extranet. To function in today’s connected economy, most companies maintain some form of connectivity with partners, suppliers, and customers.

* All of these connections are critical to the successful operation of the business and are sometimes overlooked (arguably on purpose) when it comes to security.
* However, companies are starting to take a greater interest in the security of their connectivity with their business constituents.
* Today more and more companies are performing tests against their once-trusted networks to look for vulnerabilities that may exist between partners or between them and remotely connected networks.
* This is also true when attempting to map a network.
* On more than one occasion discovery tools are used on these network segments only to find that they can see the entire network of a partner, or even worse, of an old partner that should have been disconnected a long time ago.
* 3. Intranet. Arguably, one of the more complicated aspects of ethical hacking is the internal hack.
* Intranet-based attacks can be difficult to perform given the imposed limitations, but in practice it is like a playground for testers.

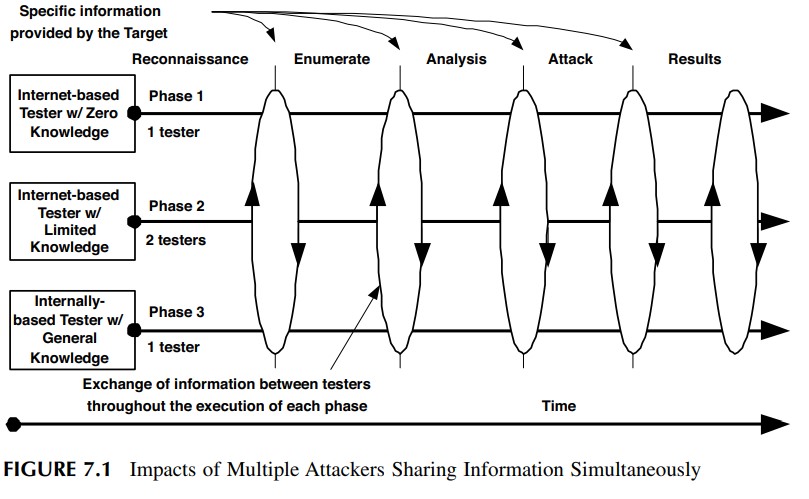
# Required Knowledge

* Usually some form of information is provided by the target and only in the most extreme cases absolutely no information is offered.
* Some cannot be avoided, such as the name of the company, whereas others can be easily kept from the testers without totally impeding the mechanics of the test.
* Following are some basic definitions of information provisioning:
* • Zero Knowledge. Zero knowledge is just that: the tester is provided nothing about the target’s network or environment.
* The tester is simply left to his ability to discover information about the client and use it to gain some form of access.
* This is also called blackbox or closed depending on who is scoping the test.
* • Limited Knowledge. Something growing in popularity with companies seeking penetration testing is providing just enough information to get started. In some cases information may include phone numbers to be tested, IP addresses, domain information, applications, and other data that would take some time to collect and do not represent any difficulty to a hacker, but are rather time consuming for the tester.
* The interesting aspect of getting some information and not all is the assumption of scope. Organizations tend to use limited information to define the boundaries of the test as opposed to providing initial data to support the engagement.
* For example, there is a difference in providing whether a customer has IDS as opposed to providing a list of phone numbers. The former is an obvious attempt to limit the information provided to the tester, whereas the latter is influencing the scope of the engagement.
* • Total Exposure. Total exposure is when every possible piece of information about the environment is provided to the tester.
* Prior to the start of the engagement, a list of questions and required items is sent to the customer in preparation for the meeting.
* At the meeting, reams of documents are provided to help the tester gain as much knowledge about the network as possible.
* This is also known as crystal box, full knowledge, or open, again depending on who is planning the engagement.

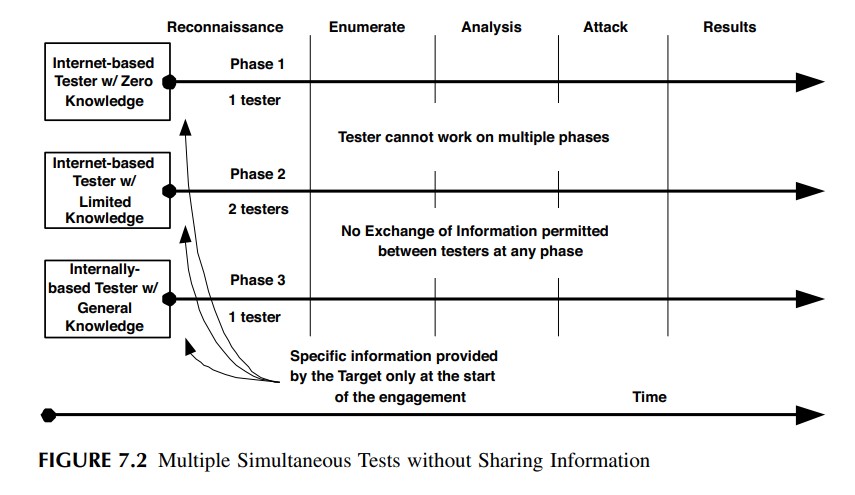
# Multi-Phased Attacks

* The following are the four types of multi phased attacks:
* 1. Parallel shared
* 2. Parallel isolated
* 3. Series shared
* 4. Series isolated

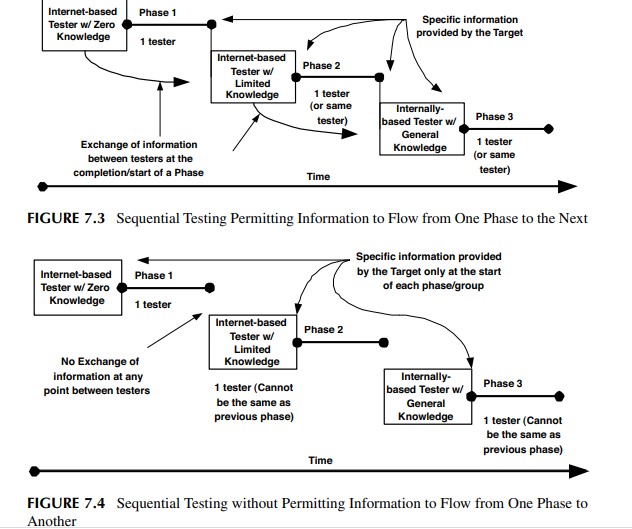
# PARALLEL SHARED



# Parallel isolated

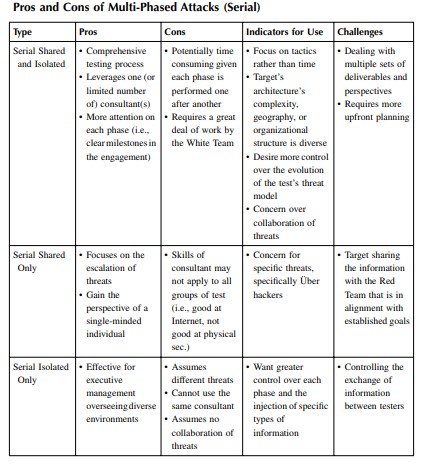


Series shared and Series isolated



# Teaming and Attack Structure

* No matter the structure of the attack, an operational protocol is crucial to the success of the test.
* As with any test there must exist procedures outside the direct experiment to ensure stability, safety, and accuracy of the results.
* There are risks that must be planned for to address the uncertainties that lie within the test itself.



# Engagement Planner

* A great number of details have been introduced: subjects ranging from multiphased attacks to information flow from the target to the testers, as well as between the testers on an engagement.
* When all these components of the test are considered, the planning of the engagement can become overwhelming.
* As stated above, many organizations have an ethical hack performed with very little planning. “Just see how far you can get,” they say.
* One of the reasons for basic forms of attack (which ultimately leads to poor value) is that planning an attack can become time consuming and arduous, putting aside the fact that many are not aware of the options available to them.
* In an effort to promote comprehensive planning on the part of the company seeking or employing an ethical hack, following are some guidelines and an example engagement planner.
* Guidelines: • Perform a self-evaluation of your goals and objectives. Ask yourself what you expect to gain from the test and how you plan to use the results. Are you looking to address specific weaknesses? Or, are you attempting to seek symptoms of a much larger problem within the security program?
* • Consider the scope of the attack and what is “in bounds.” Moreover, take the time to evaluate what you have determined is beyond its scope and the potential impact on the objectives. Too much focus of a test is typically the result of budget restrictions or departmental segmentation. With proper planning, both of these areas can be accommodated while still meeting your goals. Of course, too little focus can lead to long engagements that provide little value.
* • Ensure all the appropriate people are involved. On paper this appears obvious and simple, but internal politics and departmental rivalries introduce interesting results. There must be an owner, a leader, or primary person that ultimately sets the goals and scope of the engagement. Tests that are planned by committee will typically fail to meet objectives..
* • Commit to having a technical expert involved in the process in addition to business managers or executives. All too often, organizations plan and execute attacks without consulting their internal expertise, specifically, security experts. A technical perspective can be very beneficial to outlining the scope and depth of the attack that should be sought to meet executive goals. However, tests that are planned by only technical resources without the dedicated involvement of business management setting loftier goals will certainly affect the potential value of the test.
* • During the planning session, ask a lot of questions. However, one must keep an open mind and expect answers that conflict with personal perceptions of security. People typically ask questions they already feel they have an answer for and look to gain the perspective of the interviewee. To ensure the test meets the goals, especially when interviewing a professional organization that performs ethical hacking tests all the time, one must be cognizant of not making any predetermined conclusions

# The Right Security Consultant

* Information security consultants have experienced an interesting evolution paralleled by the expansion of technology and the proliferation of threats to which companies are regularly exposed.
* Security consultants come in many forms with different abilities and conclusions about security.
* Much of this is based on their exposure and experience in the security industry and where they have realized successes and failures.
* Nevertheless, the skill of security consultants can be categorized in two fundamental camps:
* technologists and architects.
* In addition, there are many who have mastered both and are highly valued and respected in their industry.

# Tester

* It is clear that ethical hacking can provide value to the overall assessment of an organization’s security posture and assist in developing solutions that better meet the types of vulnerabilities and threats.
* However, there is a trend for enterprises, as well as professional service firms, to hire “reformed” hackers.
* This is a likely progression of the philosophy of ethical hacking.
* Few understand the idiosyncrasies in performing a comprehensive attack; the processes are difficult to learn, and even harder to practice in the wild, where it matters most.
* It is only natural to conclude that an experienced hacker would have the necessary skills for performing hacking services.

# Logistics

* Planning takes time and effort, but it is well worth it.
* So far, we have discussed planning in the form of establishing teams, setting expectations, understanding the ultimate value of the test, and determining the impacts of various restrictions and limitations.
* There is another side to planning:
* logistics. Logistics are the nuts and bolts of an engagement and are a necessary evil to ensure the total operation is a success.
* AGREEMENTS An agreement between the service provider and the customer is a must. Many service provider organizations have a master services agreement that outlines the legal stipulations of the business relationship. These can include warrantees, guarantees, expectations of payment, and other attributes that establish an understanding of the working association. Although usually comprehensive, it is doubtful that standing agreements cover areas directly associated with the risks of hacking a network.
* AGREEMENTS An agreement between the service provider and the customer is a must.
* Many service provider organizations have a master services agreement that outlines the legal stipulations of the business relationship.
* These can include warrantees, guarantees, expectations of payment, and other attributes that establish an understanding of the working association.
* Although usually comprehensive, it is doubtful that standing agreements cover areas directly associated with the risks of hacking a network.

# Intermediates

* During a test, many networks and organizations can be caught in the wake of an attack and possibly be affected by a test to which they did not agree.
* Also, given that organizations are focused on security issues more so now than ever before, the test can raise concerns for companies that are between the tester and the target.
* It may be necessary to notify the owners of networks that have the potential of being inadvertently included in the attack.
* Partners
* As networks have evolved, companies have leveraged them to exchange information with other firms to promote more effective business models and growth through alliances.
* As with any network, there is an opportunity for the tester to infiltrate the target’s network by using an alternate route provided by a partner network
* Customers
* Businesses offer a wide range of products and services to customers that may be based on technical integration to provide the product.
* Some examples of customer interaction are very similar to the partner communications as detailed above.
* In general, businesses supply several different types of network connectivity for their customers, such as frame relay, remote dial-in access, and VPN on a segmented network, much the way they support partners.
* Conversely, many companies such as Amazon.com and Yahoo! offer products and services simply over the Internet that are accessed via a traditional Web browser
* Service Providers
* It is common for a company to use a service provider to support various IT services internally or for external customer support.
* Services can range from simple Internet connections and collaboration tools to applications and managed security services.
* An ethical hack can have a multitude of problems on these services with varying degrees of impact. Although each one can be addressed specifically, the best method is to establish a basic approach that can be applied to all types of services, if for no other reason than to build a starting point. • This can include:
* Communication. Apprise the service provider that the test is being performed and create a communication protocol to support emergencies.
* Details. The source IP addresses of the tester, timing of the test, and what falls within the scope of the test are all important elements to share with any provider.
* Support. More often than not, service providers can help with collecting information about the test. This is especially true with managed security service providers. They can passively collect information about the test and provide a report on activity.

# Law Enforcement

* law enforcement, specifically the FBI, is getting more and more involved with Internet-related attacks.
* Usually, the FBI only becomes involved after the attack to help investigate the crime in support of the victim.
* However, more time is being invested by the FBI and other law enforcement agencies in looking for malicious activities on the Internet.
* When planning an attack against a company, especially large ones that have historically attracted hackers and may have asked the FBI for support, it is important to make them aware of the test.
* Not to do so could jeopardize the engagement or the tester.
* This is especially important if there is an ongoing investigation at the target company, or a customer or partner of the company is being investigated.
* Notifying law enforcement is not necessary in most engagements, but it should be considered as a gesture of professionalism and awareness that the test could affect others inadvertently involved.

UNIT-3

# TECHNICAL PREPARATION

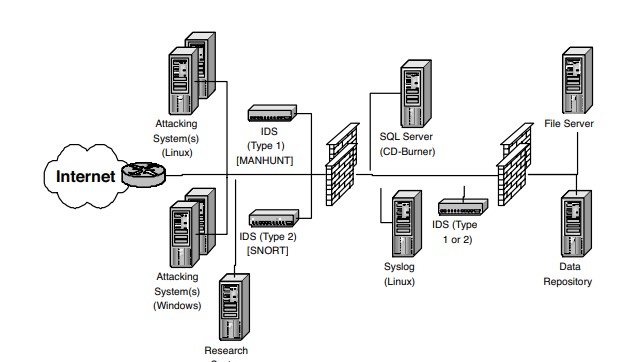
* ATTACKING SYSTEM
* Operating System
* Tools
* Data Management and Protection.
* Communications
* Operating System
* Tools
* Data Management and Protection

# THE HUNTER BECOMING THE HUNTED

* Baseline a Standard Build.
* Bootable CD
* Modified Storage • Dynamic Encryption
* E-Mail.
* Documentation
* Codenames

# ATTACKING NETWORK

* Attacking Network Architecture



* By sourcing the attack from a set of known IP addresses, the target can easily identify traffic from the tester.
* By sourcing the attack from a point deeper in the network, the potential exists for exposing internal systems to undesirable traffic.
* If the test is performed from different locations that do not have supporting systems, the likelihood of exposing the target’s data increases.
* In the event a different ISP is used that is unaware of the tester’s activities, traffic may be blocked or reported to authorities

# MANAGING THE ENGAGEMENT

* PROJECT INITIATION
* Identify Sponsors
* Building the Teams

# WHITE TEAM PROBLEMS AFFECTING THE TEST

* Shadow Consultant.
* Technical Representation • Customer Relations
* Schedule and Milestones
* Tracking
* Escalation
* Customer Approval.

# DURING THE PROJECT

• Status Reports. Monitoring

Value Scope Management.

Deliverable Review

# SOCIAL ENGINEERING

* THE PHYSICALITY OF SOCIAL ENGINEERING
* E-MAIL
* TRUSTING E-MAIL
* Value

penetration test include fraudulent e-mails can be very valuable for the following reasons:

* Inexpensive
* Knowing What’s Available.
* Security Culture
* Information Type
* Impact

# Controlling Depth

* One Shot
* Three Strikes.
* Illicit Content
* Subject Matter
* Length
* Subject

HELPDESK FRAUD

* GOOD HELPDESK PRACTICES GONE WRONG

# Value

* Protocol
* Services
* Exposure
* Inexpensive

# Controlling Depth

* Group.
* Subject.
* Number of Calls
* PROWLING AND SURFING
* INTERNAL RELATIONS AND COLLABORATION
* CORPORATE IDENTITY ASSUMPTION

# PHYSICAL SECURITY

* OBSERVATION
* DUMPSTER DIVING
* WARDRIVING AND WARCHALKING
* THEFT

# INTERNET RECONNAISSANCE

* GENERAL INFORMATION
* Web Sites
* Newsgroups
* TECHNICAL RECONNAISSANCE
* Ping Sweeps • Scans
* Passive Scan
* Active Scan
* Interactive Scan

UNIT-4

Enumeration

# ENUMERATION TECHNIQUES

* Connection Scanning
* SYN Scanning
* FIN Scanning
* Fragment Scanning
* TCP Reverse IDENT Scanning
* FTP Bounce Scanning
* UDP Scanning
* ACK Scanning

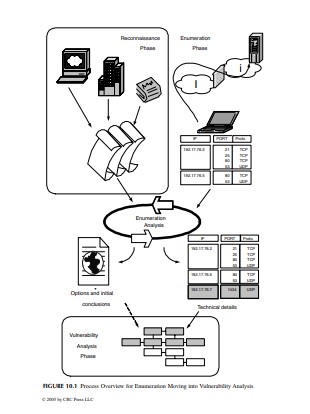
# SOFT OBJECTIVE

* LOOKING AROUND OR ATTACK?
* IS IT SCANNING OR EXPLOITATION?

# ELEMENTS OF ENUMERATION

* Account Data
* Architecture
* Operating Systems
* Wireless Networks
* Applications
* Custom Applications

# PREPARING FOR THE NEXT PHASE



# WEIGHING THE VULNERABILITY

* HACKING AN OLD HOLE IS BAD BUSINESS
* Trojans
* Today’s Hole
* Huge-Hole Syndrome
* Too Many
* Hacker Tracks

# SOURCE POINTS

* OBTAINED DATA
* THE NEEDLE IN THE HAYSTACK

# THE INTERNET

* Advisories
* Vulnerabilities
* Incidents
* Read the Manual
* Default Installs
* Default Passwords
* Hidden Accounts
* Protocol Standards

# NASTY TOOLS AND THE DIFFICULTY IN FINDING THEM

* VENDORS
* Alerts
* Service Packs

REPORTING DILEMMA

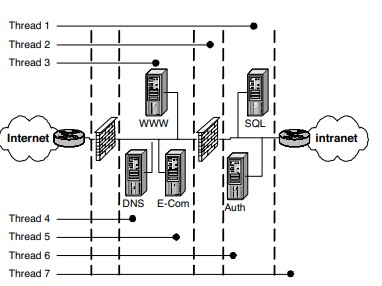
* REPORTING PROBLEMS IS NOT ALWAYS EASY

INTUITIVE TESTING

# EVASION

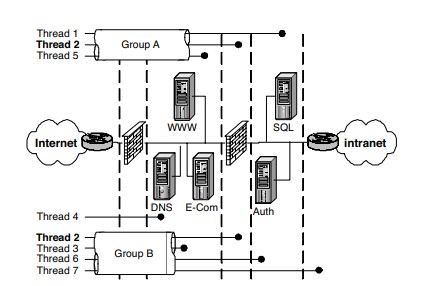
* Intrusion Detection System
* Signature Analysis.
* Protocol Analysis.
* Anomaly Detection
* Anomaly Signatures • Statistical Modeling
* Observation.
* Evasion

# THREADS AND GROUPS



* Threads 1 and 6 take the attack to the next level by interacting with the servers on the protected layer behind the inner firewalls and before the internal network. However, it should be noted that to accomplish this task (for the purposes of this demonstration) the same tactics used in thread 2 may not fully apply. In other words, to get to the SQL and authentication servers the tester would have to traverse the outer router and firewall while having enough structure left in the thread to penetrate the inner firewall. If thread 2 tactics were used, the inner firewall might thwart the attack.
* Finally, thread 7 makes it into the internal network. This could be achieved by several different tactics including false packets, manipulating one of the servers in the DMZ or inner servers, or simply taking advantage of poor security practices. Attacks that penetrate into the internal network are typically founded on gaps in the layers of applied security. These usually leverage a small opportunity in an element found in one of the outer systems and pry it open to gain greater access. Once on the internal network there are several opportunities to move deeper quickly

# GROUPS



# OPERATING SYSTEMS

* WINDOWS
* UNIX

PASSWORD CRACKERS

* ROOTKITS

# APPLICATIONS

* WEB APPLICATIONS
* DISTRIBUTED APPLICATIONS
* CUSTOMER APPLICATIONS

# WARDIALING

* One of the earliest forms of attack was using the phone system to gain access to a company’s assets. Several years ago this was an extremely successful method for attacking remote systems because prior to VPN technology most if not all remote access was provided by modems on servers or terminal devices on the company’s network
* Randomize
* After Hours
* Take Your Time
* Number Scanning
* System Type Scanning
* Banner Collection
* Brute Force

# NETWORK

* PERIMETER
* NETWORK NODES

# SERVICES AND AREAS OF CONCERN

* SERVICES
* Services Started by Default
* WINDOWS PORTS
* Null Connection
* REMOTE PROCEDURE CALLS (RPC)

# SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

• SNMP is used by network management systems to determine the “health” of a networked device. These devices range from routers and switches to servers and desktops. SNMP is a cleartext protocol as discussed earlier. The information gathered by this protocol can be used by hackers to gain valuable knowledge such as the OS version, failed hardware, the managing NMS server IP, subnet mask, and internal and external IP information. There are two “default” network paths for SNMP, public (read only) and private (read/write). Because SNMP is a default service running on your network devices (routers and switches), you can bet that unless someone changed the default community strings, they are still set to public and private. Anyone with an SNMP tool can gain the information discussed earlier via the “public” community string. If they have the “private” string they now have write access on your device and can change information, and take control if you will, of your device.

# BERKELEY INTERNET NAME DOMAIN (BIND)

• BIND is an application used to provide users and applications with domain name service. It is a very popular and common target for attacks because it is the most widely distributed DNS software and the servers running BIND are usually accessible from the Internet. Moreover, it does not help that a new vulnerability is exposed every three or four months, offering yet another form of access to attackers

# COMMON GATEWAY INTERFACE (CGI)

• CGI programs are readily available on the Internet and some companies even have internal developers to create these programs for custom Web applications. Developers are constantly challenged to include security practices when they are creating these programs. Elements such as running the programs with least-privilege or using valid buffers to prevent overflows are two examples of creating and implementing programs with slightly more resistance to attack. Another would be ensuring data arrays process their data correctly. All too often a program accepts data entry from a user, places it in an array or variable that stores the information in memory, and then proceeds to process the data without checking first if the entry was valid.

# CLEARTEXT SERVICES

• Services that use unencrypted data present another challenge for administrators. These services transmit their data in the clear, which allows anyone “watching” on the same network the ability to retrieve that information, most importantly user IDs and passwords. These two key pieces of information will be used to log in to the system the valid user attempted to log in to when the information was gathered. Services such as FTP, telnet, and e-mail are frequently used by everyday users, especially e-mail. All it takes is a hacker with a sniffer tool to easily capture this data

# NETWORK FILE SYSTEM (NFS)

• UNIX systems utilize NFS to share files and directories and drives across the network. NFS is insecure in its natural state. Most administrators allow read and write access to everyone rather than narrow down the list to a select few. The issue lies with NFS running on an Internet-facing server. This provides attackers, anyone really, with access to the files, directories, or drives on that system. The attacker is only limited to the actual permissions applied to the mounted system. Meaning, if the “world” or “other” group has write privileges, then so does your attacker. They can place any files or remove files from your NFS share. There are other vulnerabilities within an unpatched “nfsd,” the daemon that runs NFS, that gives an attacker root privileges

# DOMAIN NAME SERVICE (DNS)

• DNS does the name resolution portion of BIND. It translates a domain name into an IP address and vice versa. Applications use DNS exclusively to look up address information when they need to send information over the Internet. Without DNS, users would have to know the exact IP address every time they wanted to surf the Web or send an e-mail. DNS is critical to the Internet.

# FILE AND DIRECTORY PERMISSIONS

• Files and directories are owned by users on a system. This means for other users to access or execute these files, the owner must assign the appropriate level of permission to his files and directories. Permissions are very similar between UNIX and Windows. There are three basics: read, write, and execute. Although there are many more in Windows, UNIX offers a “special” one called “setuid/setguid.” Our three basics are self-explanatory. Read gives the owner and anyone in the group permission to “read” the file. Write gives the owner and anyone in the group permission to “write” to the file (Windows calls it modify). And last, execute gives the owner and anyone in the group permission to “execute” the file. These permissions, if not restricted, can lead to vulnerabilities

# FTP AND TELNET

• r issue with FTP is the fact that some administrators fail to remove or lock down the anonymous or guest account. These accounts, even with read-only access, can still provide some very valuable information about your system. If this service is not configured properly, administrators can give write privileges to these accounts as well, resulting in more serious consequences

# INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

• ICMP is used mainly by administrators as a quick way to determine if a server or, more appropriately, if an interface on a server is up or down. Ping provides a very simple answer and is one of the most common denial-of-service attacks. One of the first tools created to perform the denial-of-service attack is POD or ping of death. Traceroute on the Windows platform utilizes ICMP and actually provides the path a packet takes to reach that interface, usually in great detail. That detail is used by hackers to find out the IP of your firewall or Internet router

# IMAP AND POP

• Commonly used by Internet e-mail applications, these protocols allow remote users to access their e-mail over the Internet. This means ports have to be open on the firewall to permit this access. Hackers using a firewall scanning tool such as “firewalk” can determine all the open ports and using known exploits for IMAP and POP can gain access to your network and/or e-mail systems. Also remember this traffic is not usually encrypted, unless you are using SSL.

# NETWORK ARCHITECTURE

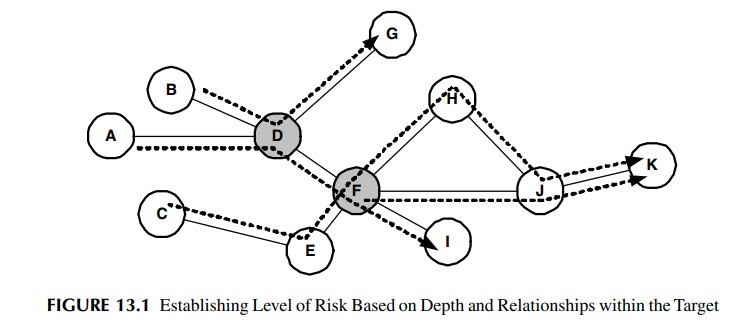
• A company may only have one DNS server used by both internal and external users. If left inside the network, external users would not be able to resolve names internal to the company without opening DNS ports on the firewall. The same holds true for internal users if the DNS resides outside the firewall. The same principle applies for e-mail users.

UNIT-5

The Deliverable

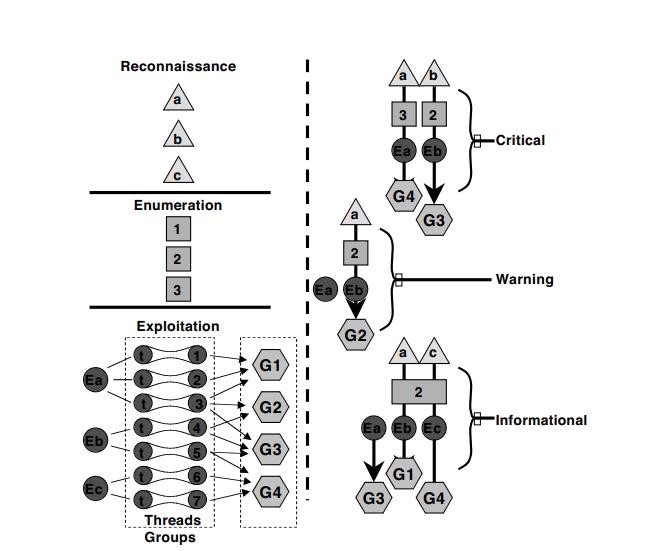
* 1. Poor Information. No interpretation is plausible because the only information in the document is a list of vulnerabilities: not very comprehensive when you consider all the intricacies of the test.
* 2. Shock Factor. Some companies are inexperienced in having tests and are shocked by the level of access the tester obtained, so much so that the entire focus is on the seemingly amazing depth the tester made into their network. Obviously, the level of success is based on hundreds of details (most introduced here) that when exposed would not be nearly as impressive. For example, it may be a shock to find that your prankster-friend sneaked into your house and stole your jewelry, until you find out that your alarm system was off and all your windows were open—kind of puts it into perspective.

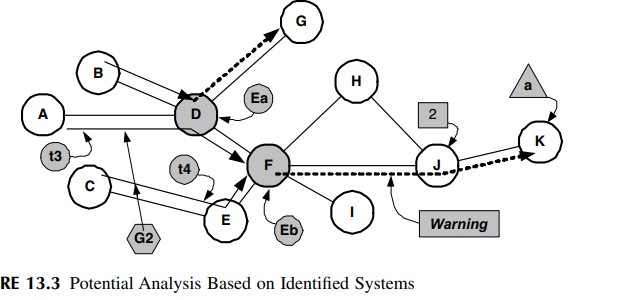
# FINAL ANALYSIS



* Critical. Critical findings are those that place the enterprise at a high degree of risk. These types of threats are usually recommended to be corrected immediately, and can often be brought to the attention of the White Team during the test. The critical classification is usually assigned to vulnerabilities that have a high threat potential in the current environment.
* Warning. A warning is representative of a threat to the company that needs to be addressed in a meaningful timeframe. It is not a risk that poses an immediate threat to the enterprise; however, it could have grave repercussions if not corrected in the near future
* Informational. Informational risks that are identified during a penetration test are those that pose a low level of risk to the organization, but in any case, need to be fixed just as the other two previously discussed. This classification of the analysis of the data collected during the penetration test is included in the final deliverable to provide additional remediation plans for the enterprise. These can sometimes include proactive measures to ensure the enterprise is protected on an ongoing basis after the penetration testing is completed. It also helps to ensure that if a third party were to come back to the enterprise, security controls would have improved within the enterprise and the same identical issues would not be discovered again

# POTENTIAL ANALYSIS





# THE DOCUMENT

* The following is an introduction to the overall format of the deliverable:
* • Executive summary
* • Present findings
* • Planning and operational summary
* • Rank vulnerabilities based on business goals and needs
* • Defining the processes and tasks employed during each phase
* • Present recommendations based on a timeline founded on risk mitigation
* • Outline any predetermined exceptions by the company
* • Final analysis and potential analysis with levels of risk in not mitigating • • Conclusion

# ALIGNING FINDINGS

* TECHNICAL MEASUREMENT
* Severity
* Exposure
* BUSINESS MEASUREMENT
* Cost
* Risk

# PRESENTATION

* REMEDIAL
* TACTICAL
* STRATEGIC

# Integrating the Results INTEGRATION SUMMARY

* 1. Mitigation.
* 2. Defense Planning.
* 3. Incident Management.

4. Security Policy

# MITIGATION

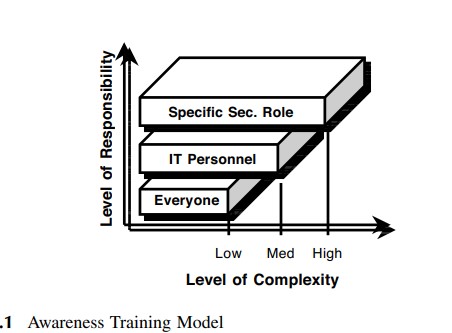
* TEST
* PILOT
* IMPLEMENT

VALIDATE

# DEFENSE PLANNING

* ARCHITECTURE REVIEW
* Architecture Review Structure • AWARENESS TRAINING

Awareness Program

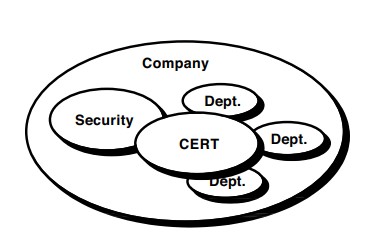


# INCIDENT MANAGEMENT

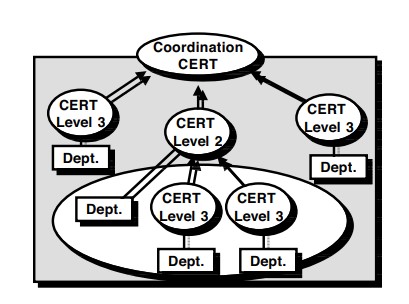
Minimize the damage from network intrusions by having a wellestablished plan in place.

* Decrease network downtime from security incidents.
* Preserve evidence from attacks.
* Increase the firm’s overall security posture and awareness
* Detect.
* Identify.
* Isolate
* Eradicate.
* Recover.
* Learn.

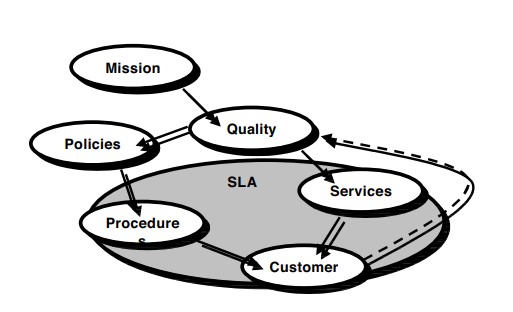
# CERT Organizational Structure



# CERT Interaction with Other Departments and CERTS within the Company



# CERT Service and Quality Framework



# Common CERT Services

* Incident Response
* Vulnerability Awareness
* Communications • Threat Analysis
* Incident Tracking
* Collaboration
* Coordination

# DATA CLASSIFICATION

* Classification Authority
* Marking
* Access Control.
* Handling Hard-Copy Documents.
* Transmission
* Storage
* Disposal.