V Skills

Skills for a secure future

Certified Ethical Hacking and Security Professional Sample Material

V-Skills Certifications

A Government of India
&
Government of NCT Delhi Initiative

V-Skills

Skills for a secure future

1. INTRODUCTION

Hacking means to “gain unauthorized access (to data in a computer)”. Hacking also describes the rapid development of new programs or the reverse engineering of already existing software to make the code better, and efficient. Hacking also refers to expand the capabilities of any electronic device; to use them beyond the original intentions of the manufacturer.

Various terms like cracker, hacker and ethical hacker are used. Hacker are persons who enjoy learning the details of computer systems and stretch their capabilities whereas, cracker is a person who uses his hacking skills for offensive purposes. Ethical hackers are usually security professionals who apply their hacking skills for defensive purposes.

There are various types of hackers as well, as described below

- ✓ White Hat Hackers - They have no malice intention and are the good guys, usually computer security experts who specialize in penetration testing and other methodologies to ensure that a company’s information systems are secure.
- ✓ Black Hat Hackers - They have malice intention and hack for malaise purposes. They break into networks or computers, or create computer viruses and always try to technologically outpace white hats. They are often called crackers as their motivation is generally to get paid.
- ✓ Gray Hat Hacker – They will break the law in the pursuit of a hack, but does not do so maliciously or for personal gain.
- ✓ Script Kiddies - They are black hat hackers who use borrowed programs to attack networks and deface websites in an attempt to make names for them.
- ✓ Spy Hackers - Corporations hire hackers to infiltrate the competition and steal trade secrets. They may hack in from the outside or gain employment in order to act as a mole. Spy hackers have the only intention to serve their client’s goals and get paid.
- ✓ State Sponsored Hackers - Governments employ hackers and hacking techniques to target enemy states to serve their military objectives online. State sponsored hackers have limitless time and funding to target civilians, corporations, and governments.
- ✓ Cyber Terrorists - They are hackers, usually motivated by religious or political beliefs, employ hacking techniques to create fear and chaos by disrupting critical infrastructures. Cyber terrorists are very dangerous, with their skills and goals.
- ✓ Hacktivists - They employ hacking techniques to expose wrongdoing or spread awareness about events or laws for political or social causes.

1.1. Ethical Hacking Evolution and Hacktivism

Ethical Hacking Evolution

The first hackers appeared in the 1960's at the Massachusetts Institute of Technology (MIT), and their first victims were electric trains. They wanted them to perform faster and more efficiently.

During the 1970's, a different kind of hacker appeared: the phreaks or phone hackers. They learned ways to hack the telephonic system and make phone calls for free. Within these group of people, a phreaker became famous because a simple discovery. John Draper, also known as Captain Crunch, found that he could make long distance calls with a whistle. He built a blue box that could do this and the Esquire magazine published an article on how to build them. Fascinated by this discovery, two kids, Steve Wozniak and Steve Jobs, decided to sell these blue boxes, starting a business friendship which resulted in the founding of Apple.

By the 1980's, phreaks started to migrate to computers, and the first Bulletin Board Systems (BBS) appeared. BBS are like the yahoo groups of today, were people posted messages of any kind of topics. The BBS used by hackers specialized in tips on how to break into computers, how to use stolen credit card numbers and share stolen computer passwords.

In 1986 the US government realized the danger due to hackers it passed the Computer Fraud and Abuse Act, making computer breaking a crime across the nation. During the 1990's, when the use of the internet widespread around the world, hackers multiplied, but it wasn't until the end of the decade that system's security became mainstream among the public and need for ethical hackers was felt.

Hacktivism

It is the act of hacking a website or computer network in an effort to convey a social or political message. It is an Internet-enabled strategy to exercise civil disobedience. The person who carries out the act of hacktivism is known as a hacktivist. Hacktivists engage in disruptive activities to highlight political or social causes. Acts of hacktivism may include website defacement, denial-of-service attacks (DoS), redirects, website parodies, information theft, virtual sabotage and virtual sit-ins. Hacktivists voice public opinions and stances regarding any repressive legislation hindering and they also educate the public on perceived regulatory injustices and encourage response.

1.2. Need and Technical Terms

Need

Due to ever evolving sophistication of cyber attacks due to well-trained, highly motivated, and well organized groups of programmers by huge criminal organizations and nation states, the need for continuous and detailed assessment of organization's security measures is essential. It is crucial for organizations to have effective infrastructure, procedures, and security policies to prevent or reduce the effects of hacking.

Hackers usually scan for weaknesses, prioritize targets and test entry points. Ethical hacking provides an objective analysis of the security systems. Ethical hacker assesses the security measures of the organization and recommends remedial steps and procedure for future prevention as well.

Technical Terms

Various technical terms used in hacking are

- ✓ Adware - It is an software that automatically generates advertisements in usually free program or like online video game. It also refers to a type of spyware that tracking browsing habits covertly to generate those ads.
- ✓ Anonymous - It is an non-hierarchical hacktivist collective, which uses hacking techniques like distributed denial of services (DDoS) attacks to register political protest in campaigns known as "#ops." Their past activity involves attacks against the Church of Scientology; Visa, Paypal, and others who withdrew their services from WikiLeaks' Julian Assange after that group began releasing war documents and #OpTunisia to support the Arab Spring. Other offshoot groups include AntiSec and LulzSec.

- ✓ Asset - An asset is any data, device, or other component of the environment that supports information-related activities that should be protected from anyone besides the people that are allowed to view or manipulate the data/information.
- ✓ Attack – It is an assault on system security and any action that violates security.
- ✓ Back door - It is also called as trap door. It is a hidden entry to a computing device or software that bypasses security measures like logins and password protections. Some have alleged that manufacturers have worked with government intelligence to build backdoors into their products. Malware is often designed to exploit back doors.
- ✓ Bot - A program that automates a usually simple action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it like hackers use bots for online content delivery, make the content calls to result in denial of service attacks.
- ✓ Botnet - A botnet is a group of computers controlled without their owners' knowledge and used to send spam or make denial of service attacks. Malware is used to hijack the individual computers, also known as "zombies," and send directions through them. They are best known in terms of large spam networks, frequently based in the former Soviet Union.
- ✓ Brute force attack – It is an automated and exhaustive key or password search for every possible instance of password. It is an inefficient method as it involves huge computing resources and used when there is no alternative.
- ✓ Clone phishing - Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.
- ✓ Code - Code is the machine-readable, usually text-based instructions that govern a device or program. Changing the code can change the behavior of the device or program.
- ✓ Compiler - A compiler is a program that translates high-level language (source code in a programming language) into executable machine language.
- ✓ Cookie - Cookies are text files sent from Web browser to a server, usually to customize information from a website.
- ✓ Denial of service attack (DoS) – It is a attack type used against a website or computer network to make it temporarily unresponsive by sending huge content requests to the site so that the server overloads.
- ✓ Distributed denial of service attack (DDoS) – It is sophisticated type of DoS using a number of separate machines to overwhelm content servers of target. It is accomplished by seeding machines with a Trojan and creating a botnet. Anonymous uses the machines of volunteers.
- ✓ Doxing - Discovering and publishing the identity of an otherwise anonymous Internet user by tracing their online publically available accounts, metadata, and documents like email accounts, as well as by hacking, stalking, and harassing.
- ✓ Exploit– A defined way to breach the security of an IT system through vulnerability. It takes advantage of vulnerability in an asset to cause unintended or unanticipated behavior in a target system, which would allow an attacker to gain access to data or information.
- ✓ Firewall - A system using hardware, software, or both to prevent unauthorized access to a system or machine.
- ✓ Hash - A hash is a number generated by an algorithm from a string of characters in a message in a communications system, the sender uses it to encrypt a message or file send it with the message. On decryption, the recipient generates another hash. If the included and the generated hash are the same, the message or file has almost certainly not been tampered with.
- ✓ IP - Internet protocol address. It's the distinctive numerical address given in four dotted numbers each can have values from 0 to 255. It identifies the device on the network, track its

activity, and discover its location. These addresses are apportioned by the regional Internet registries of the IANA (the Internet Assigned Numbers Authority).

- ✓ IRC - Internet relay chat is a protocol used by both groups and for one-on-one conversations. Often utilized by hackers to communicate or share files. Because they are usually unencrypted, hackers sometimes use packet sniffers to steal personal information from them.
- ✓ Keystroke logging - It is the tracking of keys depressions on a computer (and which touchscreen points are used) to record login IDs and passwords. Keyloggers are usually secreted onto a device using a Trojan delivered by a phishing email.
- ✓ Logic bomb - A virus secreted into a system that triggers a malicious action when certain conditions are met. The most common version is the time bomb.
- ✓ Malware - A software program designed to hijack, damage, or steal information from a device or system and includes spyware, adware, rootkits, viruses, keyloggers, and many more. The software can be delivered in a number of ways, from decoy websites and spam to USB drives.
- ✓ Master – It is the main computer in a botnet that controls, but is not controlled by, all the other devices in the network. It's also the computer to which all other devices report, sending information, such as credit card numbers, to be processed.
- ✓ Misconfigurations - Systems can also be misconfigured or left at the lowest common security settings to increase ease of use for the user, which may result in vulnerability and an attack.
- ✓ NSA – It belongs to U.S. intelligence group, The National Security Agency is dedicated to intercepting and analyzing data, specifically electronic data.
- ✓ Payload - The cargo of a data transmission is called the payload. In black hat hacking, it refers to the part of the virus that accomplishes the action, such as destroying data, harvesting information, or hijacking the computer.
- ✓ Packet sniffer - Sniffers are programs designed to detect and capture certain types of data. Packet sniffers are designed to detect packets traveling online. Packets are packages of information traveling on the Internet that contain the destination address in addition to content. Packet can be used to capture login information and passwords for a device or computer network.
- ✓ Phishing – It is a hacking technique to trick users into giving their personal information, including login information, credit card numbers, etc. by imitating legitimate companies, organizations, or people online. It is often done via fake emails or links to fraudulent websites.
- ✓ Remote access – It is the process of getting a target computer to recognize keystrokes as its own, like changing a TV with a remote control. Gaining remote access allows hackers to run the target machine completely by own, allowing for the transfer of files.
- ✓ Risk - It is defined as the impact (damage) resulting from the successful compromise of an asset. For example, an organization running a vulnerable apache tomcat server poses a threat to an organization and the damage/loss that is caused to the asset is defined as a risk. Usually, a risk is computed as Risk = Threat * vulnerabilities * impact
- ✓ Rootkit - A rootkit is a set of software programs used to gain administrator-level access to a system and set up malware, while simultaneously camouflaging the takeover.
- ✓ Security - It is a state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable levels. Security is based upon
  - ✓ Confidentiality is the concealment of information or resources.
  - ✓ Authenticity is the identification and assurance of the origin of information.
  - ✓ Integrity refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes.

  - ✓ Availability refers to the ability to use the information or resource desired
- ✓ Shrink-Wrap Code - Many off-the-shelf programs come with extra features the common user isn't aware of, and these features can be used to exploit the system. The macros in Microsoft Word, for example, can allow a hacker to execute programs from within the application.
- ✓ Social Engineering – It is an hacking technique, conning people into giving confidential information, such as passwords to their accounts. Given the difficulty of breaking, 128-bit encryption with brute force it is used and includes phishing and spear-phishing.
- ✓ Spam - Unwanted and unsolicited email and other electronic messages that attempt to convince the receiver to either purchase a product or service, or use that prospect to defraud the recipient. Spamming companies often use botnets to send spam.
- ✓ Spear-phishing – It is a type of phishing, targeting a smaller group of targets, from a department within a company or organization down to an individual.
- ✓ Spoofing - Email spoofing is altering the header of an email so that it appears to come from elsewhere like from bank. IP spoofing is the computer version, in which a packet is sent to a computer with the IP altered to imitate a trusted host in the hope that the packet will be accepted and allow the sender access to the target machine.
- ✓ Spyware - Spyware is a type of malware that is programmed to hide on a target computer or server and send back information to the master server, including login and password information, bank account information, and credit card numbers.
- ✓ Target of Evaluation – It is an IT system, product, or component that is identified or subjected as requiring security evaluation as per it's relevance.
- ✓ Threat – It is an action or event which is a potential violation of security. It represents a possible danger to the computer system. A successful exploitation of vulnerability is a threat.
- ✓ Time bomb – It is a virus whose payload is deployed at or after a certain time.
- ✓ Trojan horse – It is a type of malware that masquerades as a desirable piece of software. Under this camouflage, it delivers its payload and usually installs a back door in the infected machine.
- ✓ Virus - Self-replicating malware that injects copies of itself in the infected machine. A virus can destroy a hard drive, steal information, log keystrokes, and many other malicious activities.
- ✓ Vulnerability - A weak spot hackers can exploit to gain access to a machine. It refers to the presence of a weakness or error in design or implementation that may result in an unexpected, undesirable event compromising the security of the system.
- ✓ Whaling – It is a spear-phishing type that targets the upper management of for-profit companies, either for financial gain, or more exposure for their cause.
- ✓ Worm – It is a self-replicating, standalone malware with no reporting to a master, and it does not need to attach itself to an existing program. It often does no more than damage or ruin the computers it is transmitted to. But it's sometimes equipped with a payload, usually one that installs back doors on infected machine to make a botnet.
- ✓ Zero day exploit - A zero day attack is a previously unknown vulnerability in a system. A zero day attack is the first such use of the exploit by a cracker.

1.3. Skills Needed and Stages of Hacking

Skills Needed

Technical and personal kills are essential requirement for being an ethical hacker.

Technical skills include computing skills, being knowledgeable about computer programming, networking, web programming, database and operating systems. In-depth knowledge about targeted platforms whether Windows, Unix or Linux is also essential. Sometimes the ethical hacker is a part of a team, hired to test network and computer systems and find vulnerabilities due to specialization in specific skill set. A strong command of countermeasures to prevent attacks is also required for post-attack remedial and prevention action.

Personal skills include patience, persistence, and immense perseverance due to variable time and level of concentration needed for successful attack.

Stages of Hacking

Phases of hacking are usually summarized in distinct phases of preparation (formal contract is signed with non-disclosure and legal clause to protect the ethical hacker against any prosecution. The contract also outlines infrastructure perimeter, evaluation activities, time schedules and resources available), conduct (evaluation technical report is made after testing vulnerabilities) and conclusion (results of the evaluation is communicated to the sponsors and corrective advise is taken if needed.). Hacking can be detailed in five distinct stages which are

Reconnaissance – It is the longest phase which may last weeks or months. This phase needs variety of sources to learn and gather information about the target which includes

- ✓ Internet searches
- ✓ Social engineering
- ✓ Dumpster diving
- ✓ Domain name management/search services
- ✓ Non-intrusive network scanning

These activities cannot be easily defended against as information about an organization or business finds its way to the Internet via various routes. Employees are often easily tricked into providing tidbits of information which, over time, act to complete a complete picture of processes, organizational structure, and potential soft-spots. Computing infrastructure should not leak following information

- ✓ Software versions and patch levels
- ✓ Email addresses
- ✓ Names and positions of key personnel
- ✓ Ensure proper disposal of printed information
- ✓ Provide generic contact information for domain name registration lookups
- ✓ Prevent perimeter LAN/WAN devices from responding to scanning attempts

Scanning – After gathering enough information about working of the business and enlisting information of value, ethical hacker begins the process of scanning perimeter and internal network devices looking for weaknesses, including

- ✓ Open ports
- ✓ Open services
- ✓ Vulnerable applications, including operating systems
- ✓ Weak protection of data in transit

- ✓ Make and model of each piece of LAN/WAN equipment

Scans of perimeter and internal devices can often be detected with intrusion detection (IDS) or prevention (IPS) solutions, but not always. Possible steps to thwart such scans are

- ✓ Shutting down all unneeded ports and services
- ✓ Allow critical devices, or devices housing or processing sensitive information, to respond only to approved devices. Closely manage system design, resisting attempts to allow direct external access to servers except under special circumstances and constrained by end-to-end rules defined in access control lists
- ✓ Maintaining proper patch levels on endpoint and LAN/WAN systems

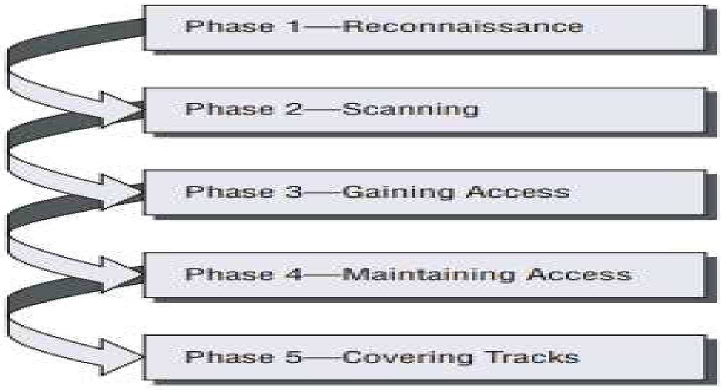
Gaining Access - Gaining access to resources is the aim of hacking attacks, either for extracting information of value or use the network as a launch site for attacks against other targets. Hence, the attacker must have some access to one or more network devices.

In addition to above defensive steps, security staff should also ensure end-user devices and servers are not easily accessible by unauthenticated users by denying local administrator access to business users and closely monitoring domain and local admin access to servers. Physical security controls also detect attempts and delay an intruder to allow effective internal or external manual response (i.e., security guards or law enforcement). Encrypting highly sensitive information and protecting keys is also crucial step to undertake. Even wit weak network security, scrambled information and denying attacker access to encryption keys is also a good defense. But other than encryption, other risks of weak security are system unavailability or use of your network in the commission of a crime.

Maintaining Access - Having gained access, an attacker must maintain access long enough to accomplish his or her objectives. Although an attacker reaching this phase has successfully circumvented your security controls, this phase can increase the attacker's vulnerability to detection. In addition to using IDS and IPS devices to detect intrusions, you can also use them to detect extrusions. The list of intrusion/extrusion detection methods includes

- ✓ Detect and filter file transfer content to external sites or internal devices
- ✓ Prevent/detect direct session initiation between servers in your data center and networks/systems not under your control
- ✓ Look for connections to odd ports or nonstandard protocols
- ✓ Detect sessions of unusual duration, frequency, or amount of content
- ✓ Detect anomalous network or server behavior, including traffic mix per time interval

Covering Tracks - After achieving the objectives of attack, the ethical hacker takes steps to hide the intrusion and possible controls left behind for future visits. Hence, other than the anti-malware, personal firewalls, and host-based IPS solutions, deny business users local administrator access to desktops. Alert on any unusual activity, any activity not expected as per the working of the business.



1.4. Ethical Hacking Modes

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

- ✓ No Knowledge Tests - No knowledge testing is also known as blackbox testing. Simply stated, the security team has no knowledge of the target network or its systems. Blackbox testing simulates an outsider attack as outsiders usually don't know anything about the network or systems they are probing. The attacker must gather all types of information about the target to begin to profile its strengths and weaknesses. The advantages of blackbox testing include

  - ✓ The test is unbiased as the designer and the tester are independent of each other.
  - ✓ The tester has no prior knowledge of the network or target being examined. Therefore there are no preset thoughts or ideas about the function of the network.
  - ✓ A wide range of resonances work and are typically done to footprint the organization, which can help identify information leakage.
  - ✓ The test examines the target in much the same way as an external attacker.

  The disadvantages of blackbox testing include
  - ✓ It can take more time to perform the security tests.
  - ✓ It is usually more expensive as it takes more time to perform.
  - ✓ It focuses only on what external attackers see, while in reality, most attacks are launched by insiders.

- ✓ Full Knowledge Testing (or Whitebox) - Whitebox testing takes the opposite approach of blackbox testing. This form of security test takes the premise that the security tester has full knowledge of the network, systems, and infrastructure. This information allows the security tester to follow a more structured approach and not only review the information that has been provided but also verify its accuracy. So, although blackbox testing will typically spend more time gathering information, whitebox testing will spend that time probing for vulnerabilities.

- ✓ Partial Knowledge Testing (or Graybox) - In the world of software testing, graybox testing is described as a partial knowledge test EC-Council literature describes graybox testing as a form of internal test. Therefore, the goal is to determine what insiders can access. This form of test might also prove useful to the organization as so many attacks are launched by insiders.

1.5. Networking Basics

A network is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information.

Networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software. A host device on a network can be computers, servers, laptops, Personal Digital Assistants (PDAs), or anything a person uses to access the network. Network devices are hubs, repeaters, bridges, switches, router and firewall.

Layered Network Model

The layered network model defines a networking framework for implementing protocols in different layers. Control is passed from one layer to the next, starting at the top most layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

The International Standards Organization (ISO) defined a seven-layer model to standardize networking processes. The benefits to layering networking protocol specifications are many including

- ✓ Interoperability - Greater interoperability between devices from different manufacturers and between different generations of same type of device from the same manufacturer.
- ✓ Compatibility - Compatibility between devices, systems and networks that this delivers.
- ✓ Better Flexibility - Improved flexibility in options and choices for configuration and installation.
- ✓ Increased Life Expectancy - Devices from different technology generations can co-exist thus the older units do not get discarded immediately newer technologies are adopted.
- ✓ Scalability - Experience shows that a layered design scales better than the horizontal approach.
- ✓ Value Added Features - It is easier to add and implement value added features into products or services when the entire system has been built on the use of a layered philosophy.
- ✓ Modularity Plug-ins and add-ons are easily added from use of a layered approach.
- ✓ Standardization and Certification –The layered design specifications facilitate streamlined and simple standardization and certification process due to the clearer and more distinct definition.
- ✓ Portability - Layered networking protocols are much easier to port from one system to another.
- ✓ Compartmentalization of Functionality – It gives freedom to concentrate on a specific layer or specific functions without the need for concern or modification of any other layer.

TCP/IP Protocol Architecture

TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. The TCP/IP model and related protocols are maintained by the (IETF) or Internet Engineering Task Force. The Internet protocol suite and the layered protocol stack design were in use before the OSI model was established. It has four abstraction layers, each with its own protocols. It has four abstraction layers, each with its own protocols. From highest to lowest, the layers are

- ✓ **Application layer (process-to-process)-** It contains all protocols (like HTTP) for specific data communications services on a process-to-process level (for example how a web browser communicates with a web server). This is the scope within which applications create user data and communicate this data to other processes or applications on another or the same host. The communications partners are often called peers. This is where the "higher level" protocols such as SMTP, FTP, SSH, HTTP, etc. operate.
- ✓ **Transport layer (host-to-host)-** It handles host-to-host communication. The transport layer constitutes the networking regime between two network hosts, either on the local network or on remote networks separated by routers. The transport layer provides a uniform networking interface that hides the actual topology (layout) of the underlying network connections. This is where flow-control, error-correction, and connection protocols exist, such as TCP. This layer deals with opening and maintaining connections between Internet hosts.
- ✓ **Internet layer (internetworking)-** It connects local networks, thus establishing internetworking. The internet layer has the task of exchanging datagrams across network boundaries. It is therefore also referred to as the layer that establishes internetworking, indeed, it defines and establishes the Internet. This layer defines the addressing and routing structures used for the TCP/IP protocol suite. The primary protocol in this scope is the Internet Protocol, which defines IP addresses. Its function in routing is to transport datagrams to the next IP router that has the connectivity to a network closer to the final data destination.
- ✓ **Link layer-** The link layer (commonly Ethernet) contains communication technologies for a local network. This layer defines the networking methods within the scope of the local network link on which hosts communicate without intervening routers. This layer describes the protocols used to describe the local network topology and the interfaces needed to affect transmission of Internet layer datagrams to next-neighbor hosts.

Application, Transport, Internet and Network Access Layer

Application Layer

It contains all protocols and methods of process-to-process communications across an Internet Protocol (IP) network. Its methods use the underlying transport layer protocols to establish host-to-host connections. Both TCP/IP and the OSI model specify a group of protocols and methods identified by the name application layer. The following protocols are described in the application layer of the Internet protocol suite.

- ✓ Remote login - Telnet
- ✓ File transfer - FTP, TFTP
- ✓ Electronic mail - SMTP,IMAP, POP
- ✓ Support services - DNS, RARP, BOOTP, SNMP

Transport Layer

The transport layer or layer 4 provides end-to-end communication services for applications by providing services like connection-oriented data stream support, reliability, flow control, and multiplexing. It is contained in the TCP/IP as TCP and in the OSI model as transport layer.

The Transmission Control Protocol (TCP) is used for connection-oriented transmissions, whereas the connectionless User Datagram Protocol (UDP) is used for simpler messaging transmissions. TCP has stateful design for reliable transmission and data stream services. Various services provided by a transport-layer protocol include

- ✓ Connection-oriented communication- Interpreting the connection as a data stream provides benefits to applications.
- ✓ Byte orientation- It is easier to process data stream as a sequence of bytes helping various underlying message formats.
- ✓ Same order delivery- The network layer doesn't guarantee data packet arrival in the same order that they were sent, hence segment numbering is used, with the receiver passing them to the application in order.
- ✓ Reliability- Packets may be lost due to network congestion hence, an error detection code like checksum checks data corruption, and verify correct receipt by sending an ACK or NACK message to sender. Automatic repeat request retransmits lost or corrupted data.
- ✓ Flow control- The rate of data transmission between two nodes is managed to prevent a fast sender for more data. It also improves efficiency by reducing buffer under run.
- ✓ Congestion avoidance- It controls traffic entry into a network by avoiding oversubscription of link capabilities of intermediate nodes and networks by reducing rate of sending packets.
- ✓ Multiplexing- Ports provide multiple endpoints on a single PC like the name on a postal address is a multiplexing, and differs between different recipients at same location. Computer applications each listen for information on their own ports, which enables the use of more than one network service at the same time.

Internet Layer or IP Layer

It is a group of internetworking methods, protocols, and specifications used to transport datagrams (packets) from the originating host across network, to destination host specified by a network address (IP address). It facilitates internetworking or connecting multiple networks by gateways.

Internet-layer protocols use IP-based packets and have three functions, for outgoing packets, select the next-hop host (gateway) and transmit the packet to this host by passing it to the appropriate link layer implementation; for incoming packets, capture packets and pass the packet payload up to the appropriate transport-layer protocol, if appropriate. In addition it provides error detection and diagnostic capability. The Version 4 of the IP (IPv4), IP is capable of automatic fragmentation or de-fragmentation of packets, based on the maximum transmission unit (MTU) of link elements.

It is not responsible for reliable transmission and offers "best effort" delivery hence, no proper arrival making network resilient and assigning reliability provision to higher level protocols. In IPv4 (not IPv6), a checksum is used to protect the header of each datagram.

Network Access Layer

It is the lowest layer which provides the means for the system to deliver data to the other devices on a directly attached network. It defines how to use the network to transmit data and thus, must know the details of the underlying network to correctly format the data being transmitted to comply with the network constraints. The TCP/IP Network Access Layer has the functions of all three lower layers of OSI (Network, Data Link, and Physical).

Functions performed at this level include encapsulation of IP datagrams into the frames transmitted by the network, and mapping of IP addresses to the physical addresses used by the network. One of TCP/IP's strengths is its universal addressing scheme. The IP address must be converted into an address appropriate for physical network over which the datagram is transmitted.

Devices at different layers

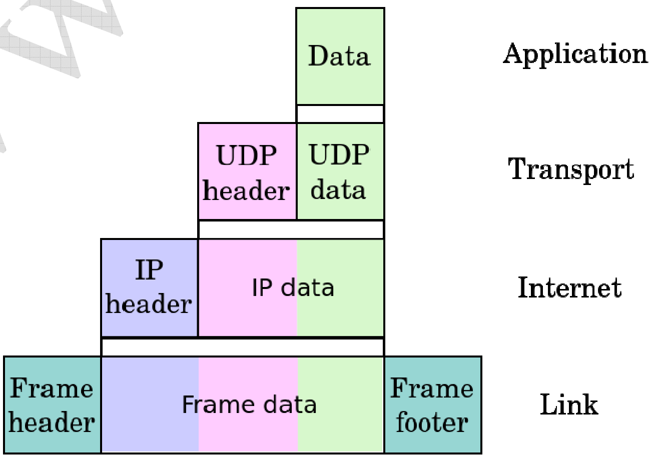
Devices at different layers of TCP/P network model are

- ✓ Layer 1- It is the physical layer. Media converters operate at Layer 1 to convert electrical signals and physical media without doing anything to data coming through the link. Media converters have two ports—one in, one out— to convert the incoming electrical signal from one cable type and then transmit it over another type.
- ✓ Layer 2- It is the data-link layer. Switch and media converter operate at Layer 2 to sort packets using physical network addresses or MAC addresses. All network hardware is permanently assigned this number during its manufacture. Both switches and media converters can be Layer 2 devices. A switch has more ports than a media converter. Devices are fast, but aren't smart as they don't look at data packets closely.
- ✓ Layer 3- It is the Network Layer and layer 3 switches use network or IP addresses to identify locations on the network. Layer 3 switches are smarter due to routing functions to find the best way to send a packet to its destination.
- ✓ Network Router - A router routes data packets between two networks by reading the destination information in each packet so, for an immediate network it has access to, it will strip the outer packet, readdress the packet to the proper Ethernet address, and transmit it but, for another network destination it is sent to another router, re-package outer packet to receive by next router and send it to next router.

Data Encapsulation

It is a method for communication protocols to logically separate functions in the network and abstracts it from their underlying structures by inclusion or information hiding within higher level objects. Link encapsulation by the physical layer allows local area networking by higher layers and IP provides global addressing of individual computers; UDP adds application or process selection, i.e., the port specifies the service such as a Web or TFTP server.

The more abstract layer is called the upper layer protocol while the more specific layer is called the lower layer protocol. Encapsulation is a characteristic feature of most networking models, including the OSI Model and TCP/IP suite of protocols. An image of encapsulation of application data descending through the layers



The OSI Reference Model

The OSI or Open System Interconnection reference model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at application layer in source and to bottom layer, over channel to destination and back up hierarchy.

Application (Layer 7)

It supports application and end-user processes. Communication destination is identified, quality of service found, user authentication and privacy are considered and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level.

Presentation (Layer 6)

It provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. It transforms data into the form that the application layer can accept by formatting and encrypting data to be sent across a network so, providing freedom from compatibility problems. It is also called the syntax layer.

Session (Layer 5)

It establishes, manages and terminates connections between applications. It sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

Transport (Layer 4)

It provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

Network (Layer 3)

It provides switching and routing technique, creates logical paths called virtual circuits to transmit data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

Data Link (Layer 2)

In it data packets are encoded and decoded into bits. It handles errors in the physical layer, flow control and frame synchronization. It is divided into two sub layers of Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

Physical (Layer 1)

It transmits the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

OSI Layers and Their Functions

Physical Layer

It is the lowest layer of the OSI model and is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to physical medium, and carries signals for all higher layers. It provides

- ✓ Data encoding - modifies digital signal (1s and 0s) of PC to characteristics of physical medium, and to aid in bit and frame synchronization like signal state for a binary 1, "bit-time" starts, etc.
- ✓ Transmission technique - determines whether the encoded bits will be transmitted by base band (digital) or broadband (analog) signaling.
- ✓ Physical medium transmission - transmits bits as electrical or optical signals appropriate for the physical medium.

Data Link Layer

It gives error-free data frames transfer from one node to another over the physical layer, allowing top layers an error-free transmission over the link. The data link layer provides

- ✓ Link establishment and termination - establishes and terminates logical link between two nodes.
- ✓ Frame traffic control - tells sender to "back-off" when no frame buffers are available.
- ✓ Frame sequencing - transmits/receives frames sequentially.
- ✓ Frame acknowledgment - provides/expects frame acknowledgments. Detects and recovers from physical layer errors by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- ✓ Frame delimiting - creates and recognizes frame boundaries.
- ✓ Frame error checking - checks received frames for integrity.
- ✓ Media access management - determines when the node "has the right" to use the physical medium.

Network Layer

It controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides

- ✓ Routing - routes frames among networks.
- ✓ Subnet traffic control - routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
- ✓ Frame fragmentation - if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
- ✓ Logical-physical address mapping - translates logical addresses, or names, into physical addresses.
- ✓ Subnet usage accounting – It has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

This layer builds headers and uses them to route data to the destination address thus, relieving upper layers. It establishes, maintains and terminates connections across communications subnet.
Peer protocols also exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station.

Transport Layer

It ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from concern of data transfer. In a reliable network layer with virtual circuit capability, a minimal transport layer is required but, unreliable one only supporting datagrams, the transport protocol should include extensive error detection and recovery. The transport layer provides

- ✓ Message segmentation - splits received message into smaller units, and passes down to the network layer. The transport layer at the destination station reassembles the message.
- ✓ Message acknowledgment - provides reliable end-to-end message delivery with acknowledgments.
- ✓ Message traffic control - tells the source to "back-off" when no message buffers are available.
- ✓ Session multiplexing - multiplexes several message streams, or sessions onto one logical link.

There are strict message size limits imposed by the network (or lower) layer so, the transport layer must break up the messages into smaller units, or frames, with a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries.

The transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source carries on a conversation with similar software on the destination by using message headers and control messages.

Session Layer

It allows session establishment between processes running on different nodes. It provides

- ✓ Session establishment, maintenance and termination - allows two application processes on different machines to establish, use and terminate a connection, called a session.
- ✓ Session support - performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

Presentation Layer

The presentation layer formats the data to be presented to the application layer. This layer may translate data from a format used by the application layer into a common format at the source then, translate the common format to a format known to application layer at destination. The presentation layer provides

- ✓ Character code translation - like, ASCII to EBCDIC.
- ✓ Data conversion - bit order, CR-CR/LF, integer-floating point, and so on.
- ✓ Data compression - reduces the number of bits that need to be transmitted on the network.
- ✓ Data encryption - encrypt data for security purposes. like, password encryption.

Application Layer

It serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions

- ✓ Resource sharing and device redirection
- ✓ Remote file access
- ✓ Remote printer access
- ✓ Inter-process communication
- ✓ Network management
- ✓ Directory services
- ✓ Electronic messaging (such as mail)
- ✓ Network virtual terminals

1.6. Penetration Testing

Planning

It is a process of creating one or more detailed plans to achieve optimum balance of demands with the available resources. The planning process involves following actions in sequence –

- ✓ Identifies the goals or objectives to be achieved
- ✓ Formulates strategies to achieve them
- ✓ Arranges or creates the means required
- ✓ Implements, directs, and monitors all steps in their proper sequence.

Planning an hacking attack evaluates existing business 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. Arguably, the planning phase of a penetration test will have a profound influence on how the test is performed and the information shared and collected, and will directly influence the deliverable and integration of the results into the security program.

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.

Maintain Anonymity

Anonymity is the quality or state of being unknown or unacknowledged.

Various techniques are used for being anonymous which usually includes

- ✓ Hacking and using open or unsecured wireless networks usually in residential buildings
- ✓ Making use of anonymous or disposable e-mail accounts from free e-mail services
- ✓ Using infected computers or zombies or bots (at other organizations)
- ✓ Using borrowed or stolen remote desktop and VPN accounts
- ✓ Using public computers at libraries, schools, etc.
- ✓ Using internet proxy servers or anonymizer services

- ✓ Workstations or servers on the victim's own network

Goal setting

- ✓ Define more specific goals. Align these goals with your business objectives. What are you and the management trying to get from this process? What performance criteria will you use to ensure you're getting the most out of your testing?
- ✓ Create a specific schedule with start and end dates as well as the times your testing is to take place. These dates and times are critical components of your overall plan.

Target System Identification

You might decide which systems to test based on a high-level risk analysis, answering questions such as

- ✓ What are your most critical systems? Which systems, if accessed without authorization, would cause the most trouble or suffer the greatest losses?
- ✓ Which systems appear most vulnerable to attack?
- ✓ Which systems crash the most?
- ✓ Which systems are not documented, are rarely administered, or are the ones you know the least about?

After you've established your overall goals, decide which systems to test. This step helps you define a scope for your ethical hacking so that you establish everyone's expectations up front and better estimate the time and resources for the job. The following list includes devices, systems, and applications that you may consider performing your hacking tests on

- ✓ Routers and switches
- ✓ Firewalls
- ✓ Wireless access points
- ✓ Web, application, and database servers
- ✓ E-mail and file servers
- ✓ Mobile devices (such as phones and tablets) that store confidential information
- ✓ Workstation and server operating systems

Attack Tree Analysis

Attack tree provides a way for modeling goals of an attack and alternative ways to achieve that goal. This helps us to study the system from the attackers' point of view, which may lead us to determine possible ways that the system can be compromised. By assigning cost or probability measures to the nods of attack tree, one can analyze if the attackers efforts worth the value that can be achieved or not, and as a result, this helps analyzing if the system is at risk and vulnerable.

Attack trees are multi-leveled diagrams consisting of one root, leaves, and children. From the bottom up, child nodes are conditions which must be satisfied to make the direct parent node true; when the root is satisfied, the attack is complete. Each node may be satisfied only by its direct child nodes.

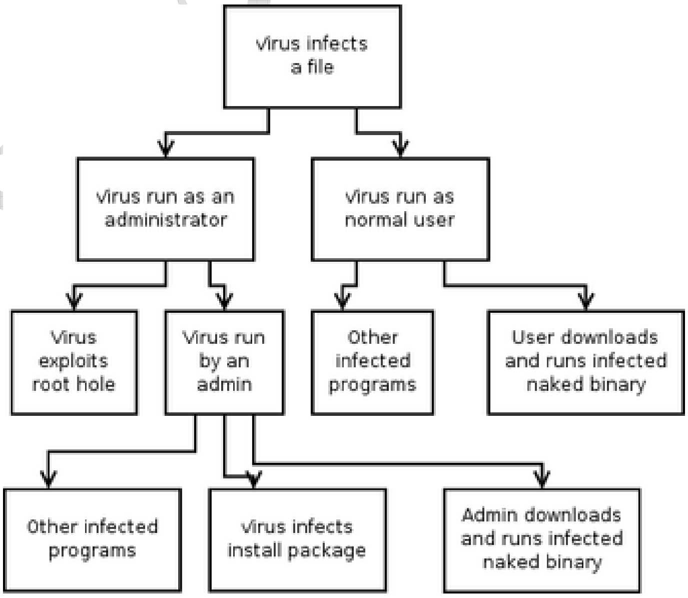
A node may be the child of another node; in such a case, it becomes logical that multiple steps must be taken to carry out an attack. For example, consider classroom computers which are secured to the desks. To steal one, the securing cable must be cut or the lock unlocked. The lock may be unlocked by picking or by obtaining the key. The key may be obtained by threatening a key holder, bribing a keyholder, or taking it from where it is stored (e.g. under a mousemat). Thus a four level attack tree can be drawn, of which one path is (Bribe Keyholder,Obtain Key,Unlock Lock,Steal Computer).

Note also that an attack described in a node may require one or more of many attacks described in child nodes to be satisfied. Our above condition shows only OR conditions; however, an AND condition can be created, for example, by assuming an electronic alarm which must be disabled if and only if the cable will be cut. Rather than making this task a child node of cutting the lock, both tasks can simply reach a summing junction. Thus the path ((Disable Alarm,Cut Cable),Steal Computer) is created.

Attack trees can become largely complex, especially when dealing with specific attacks. A full attack tree may contain hundreds or thousands of different paths all leading to completion of the attack. Even so, these trees are very useful for determining what threats exist and how to deal with them.

Attack trees can lend themselves to defining an information assurance strategy. It is important to consider, however, that implementing policy to execute this strategy changes the attack tree. For example, computer viruses may be protected against by refusing the system administrator access to directly modify existing programs and program folders, instead requiring a package manager be used. This adds to the attack tree the possibility of design flaws or exploits in the package manager.

Attack tree for computer viruses. Here we assume a system such as Windows NT, where not all users have full system access. All child nodes operate on OR conditions.


Virus infects a file
Virus run as an administrator
Virus run as normal user
Virus exploits root hole
Virus run by an admin
Other infected programs
User downloads and runs infected naked binary
Other infected programs
Virus infects install package
Admin downloads and runs infected naked binary

Structuring, Executing and Reporting Penetration Test

Creating Testing Standards

One miscommunication or slip-up can send the systems crashing during your ethical hacking tests. No one wants that to happen. To prevent mishaps, develop and document testing standards. These standards should include

✓ When the tests are performed, along with the overall timeline
✓ Which tests are performed
✓ How much knowledge of the systems you acquire in advance
✓ How the tests are performed and from what source IP addresses (if performed across the Internet)
✓ What you do when a major vulnerability is discovered

Timing

Make sure that the tests you perform minimize disruption to business processes, information systems, and people. You want to avoid harmful situations such as mis-communicating the timing of tests and causing a DoS attack against a high-traffic e-commerce site in the middle of the day or performing password-cracking tests in the middle of the night. It's amazing what a 12-hour time difference (2 p.m. during major production versus 2 a.m. during down time) can make when testing your systems! Even having people in different time zones can create issues. Everyone on the project needs to agree on a detailed timeline before you begin. Having the team members' agreement puts everyone on the same page and sets correct expectations.

If possible and practical, notify your Internet service providers (ISPs) or hosting collocation providers. These providers have firewalls or intrusion detection systems (IDS) or intrusion prevention systems (IPS) in place to detect malicious behavior. If your provider knows you're conducting tests, it's less likely to block your traffic.

Running specific tests

You might have been charged with performing a general penetration test, or you may want to perform specific tests, such as cracking passwords or trying to gain access to a web application. Or you might be performing a social engineering test or assessing Windows on the network. However you test, you might not want to reveal the specifics of the testing. Even when your manager or client doesn't require detailed records of your tests, document what you're doing at a high level. Documenting your testing can help eliminate any potential miscommunication and keep you out of hot water.

Enabling logging on the systems you test along with the tools you use provides evidence of what and when you test and more. It may be overkill, but you could even record screen actions using a tool such as TechSmith's Camtasia Studio (www.techsmith.com/camtasia.html). Sometimes, you might know the general tests that you perform, but if you use automated tools, it may be next to impossible to understand every test you perform completely. This is especially true when the software you're using receives real-time vulnerability updates and patches from the vendor each time you run it. The potential for frequent updates underscores the importance of reading the documentation and readme files that come with the tools you use.

An updated program once bit me. I was performing an automated assessment on a client's website – the same test I performed the previous week. The client and I had scheduled the test date and time in advance. But I didn't know that the software vendor made some changes to its web form submission tests, and I accidentally flooded the client's web application, creating a DoS condition.

Blind versus knowledge assessments

Having some knowledge of the systems you're testing might be a good idea, but it's not required. But, a basic understanding of the systems you hack can protect you and others. Obtaining this knowledge shouldn't be difficult if you're hacking your own in-house systems. If you hack a client's systems, you might have to dig a little deeper into how the systems work so you're familiar with them. Doing so has always been my practice and I've only had a small number of clients ask for a full blind assessment because most people are scared of them. This doesn't mean that blind assessments aren't valuable, but the type of assessment you carry out depends on your specific needs.

The best approach is to plan on unlimited attacks, wherein any test is possible, possibly even including DoS testing. The bad guys aren't poking around on your systems within a limited scope, so why should you?

Picking your location

The tests you perform dictate where you must run them from. Your goal is to test your systems from locations accessible by malicious hackers or employees. You can't predict whether you'll be attacked by someone inside or outside your network, so cover all your bases. Combine external (public Internet) tests and internal (private network) tests.

You can perform some tests, such as password cracking and network-infrastructure assessments, from your office. For external hacks that require net-work connectivity, you might have to go off-site (a good excuse to work from home) or use an external proxy server. Some security vendors' vulnerability scanners (such as QualysGuard) are run from the cloud, so that would work as well. Better yet, if you can assign an available public IP address to your computer, simply plug in to the network on the outside of the firewall for a hacker's-eye view of your systems. Internal tests are easy because you need only physical access to the building and the network. You might be able to use a DSL line or cable modem already in place for visitors and similar users.Responding to vulnerabilities you find

Determine ahead of time whether you'll stop or keep going when you find a critical security hole. You don't need to keep hacking forever or until you crash all the systems. Just follow the path you're on until you just can't hack it any longer (pardon the pun). When in doubt, the best thing to do is to have a specific goal in mind and then stop when that goal has been met.

Selecting Security Assessment Tools

Which security assessment tools you need depend on the tests you're going to run. You can perform some ethical hacking tests with a pair of sneakers, a telephone, and a basic workstation on the network, but comprehensive testing is easier with hacking tools.

It's important to know what each tool can and can't do and how to use each one. I suggest reading the manual and other Help files. Unfortunately, some tools have limited documentation, which can be frustrating. You can search forums and post a message if you're having trouble with a tool.

Hacking tools can be hazardous to your network's health. Be careful when you use them. Always make sure that you understand what every option does before you use it. Try your tools on test systems if you're not sure how to use them. These precautions help prevent DoS conditions and loss of data on your production systems.

Setting the Stage for Testing

In the past, a lot of ethical hacking involved manual processes. Now, certain vulnerability scanners can automate various tasks, from testing to reporting to remediation validation (the process of determining whether a vulnerability was fixed). These tools allow you to focus on performing the tests and less on the specific steps involved. However, following a general methodology and understanding what's going on behind the scenes will help you.

Ethical hacking is similar to beta testing software. Think logically — like a programmer, a radiologist, or a home inspector — to dissect and interact with all the system components to see how they work. You gather information, often in many small pieces, and assemble the pieces of the puzzle. You start at point A with several goals in mind, run your tests (repeating many steps along the way), and move closer until you discover security vulnerabilities at point B.

The process used for ethical hacking is basically the same as the one a malicious attacker would use. The primary differences lie in the goals and how you achieve them. Today's attacks can come from any angle against any system, not just from the perimeter of your network and the Internet as you might have been taught in the past. Test every possible entry point, including partner, vendor, and customer networks, as well as home users, wireless LANs, and mobile devices. Any human being, computer system, or physical component that protects your computer systems — both inside and outside your buildings — is fair game for attack.

When you start rolling with your ethical hacking, keep a log of the tests you perform, the tools you use, the systems you test, and your results. This information can help you do the following - track what worked in previous tests and why.

Help prove what you did.

Correlate your testing with intrusion detection systems (IDSs) and other log files if trouble or questions arise.

Document your findings.

In addition to taking general notes, taking screen captures (using Snagit or a similar tool) of your results whenever possible is very helpful. These shots come in handy later should you need to show proof of what occurred, and they also will be useful as you generate your final report. Also, depending on the tools you use, these screen captures might be your only evidence of vulnerabilities or exploits when it comes time to write your final report.