**UNIT 2**

1. **What is DDoS? Illustrate with example.**

* DDoS Attacks:

The most common form of DoS attack today is the DDoS attack. This is accomplished by getting various machines to attack the target. A typical way this is done is by sending out a Trojan horse that will cause infected computers to attack a specified target at a particular date and time. This is a very effective way to execute a DDoS attack on any target. In this form of attack, the attacker does not have direct control of the various machines involved. These machines are simply infected by some malware that causes them to participate in the attack on a particular date and time.

Another method is to use a botnet to orchestrate the attack. Botnets are networks of computers that have been compromised by the attacker, giving said attacker control of the infected system. This is often accomplished via delivery of a Trojan horse. However, unlike with the form of DDoS attack just mentioned, the attacker has direct control of the attacking machines in the botnet.

// Draw DDOS diagram yourself which you studied last year ~Aditya Madur~

Real-World Examples of DoS Attacks:

Boston Globe Attack: On November 8, 2017, the Boston Globe was hit with a large-scale DDoS attack against bostonglobe.com and other websites owned by the company. The attack also interrupted the company’s telephones. The attack was only stopped by the company’s Internet service provider implementing anti-DDoS measures, such as throttling bandwidth.

Memcache Attacks: In February 2017 a new DDoS attack vector emerged. Attackers used memcache, a database caching system, to amplify traffic volume. A request could be amplified by a factor of several thousand by using this method. The aforementioned GitHub attack involved memcaching.

**UNIT 4**

1. **What is Digital Signature? How it works? *(// Optional)***

🡺 A digital signature is not used to ensure the confidentiality of a message but rather to guarantee who sent the message. This is referred to as nonrepudiation. Essentially, nonrepudiation means proving who the sender is. Digital signatures are rather simple, but they are clever. They simply reverse the asymmetric encryption process.

Recall that in asymmetric encryption, the public key (which anyone can have access to) is used to encrypt a message to the recipient, and the private key (which is kept secure and private) can decrypt it. With a digital signature, the sender encrypts something with his private key. If the recipient can decrypt that with the sender’s public key, then it must have been sent by the person purported to have sent the message. This process is shown in Figure:

A diagram of a signature

Description automatically generated

1. **What is firewall? Explain types of firewalls.**

🡺 There are numerous types of firewalls and variations on those types. But most firewalls can be grouped into one of the following three families of firewalls: Packet inspection, Stateful packet inspection, Application Gateways.

1. Packet Filtering:

Basic packet filtering is the simplest form of firewall. It involves looking at packets and checking to see if each packet meets the firewall rules. For example, it is common for a packet filtering firewall to consider three questions:

Is this packet using a protocol that the firewall allows?

Is this packet destined for a port that the firewall allows?

Is the packet coming from an IP address that the firewall has not blocked?

These are three very basic rules. Some packet filter firewalls check additional rules. But what is not checked is the preceding packets from that same source. Essentially, each packet is treated as a singular event, without reference to the preceding conversation. This makes packet filtering firewalls quite susceptible to some DoS attacks, such as SYN floods.

1. Stateful Packet Inspection:

Any stateful packet inspection (SPI) firewall will examine each packet and deny or permit access based not only on the examination of the current packet but also on data derived from previous packets in the conversation. The firewall is therefore aware of the context in which a specific packet was sent. This makes such a firewall far less susceptible to ping floods and SYN floods, as well as less susceptible to spoofing. For example, if a firewall detects that the current packet is an ICMP packet and a stream of several thousand packets have been continuously coming from the same source IP, the firewall will see that this is clearly a DoS attack, and it will block the packets. A stateful packet inspection firewall can also look at the actual contents of a packet, which allows for some very advanced filtering capabilities. Most high-end firewalls use the stateful packet inspection method; when possible, this is the recommended type of firewall.

1. Application Gateways:

An application gateway (also known as application proxy or application-level proxy) is a program that runs on a firewall. When a client program, such as a web browser, establishes a connection to a destination service, such as a web server, it connects to an application gateway, or proxy. The client then negotiates with the proxy server in order to gain access to the destination service. In effect, the proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on the network behind the firewall. This process actually creates two connections. There is one connection between the client and the proxy server, and there is another connection between the proxy server and the destination.

Once a connection is established, the application gateway makes all decisions about which packets to forward. Since all communication is conducted through the proxy server, computers behind the firewall are protected.

Essentially, an application firewall is used for specific types of applications, such as database or web server applications. It is able to examine the protocol being used (such as HTTP) for any anomalous behaviour and block traffic that might get past other types of firewalls. It is common to have an application firewall that also includes stateful packet inspection.

1. **Explain the following:**

**1) Snort:**

Several vendors supply IDSs, and each has unique strengths and weaknesses. Which system is best for your environment depends on many factors, including the network environment, security level required, budget constraints, and skill level of the person who will be working directly with the IDS. One popular open-source IDS is Snort, which can be downloaded for free from [www.snort.org](http://www.snort.org).

While it is not the only IDS available, it is free, and that makes it an attractive option for many people.

Snort is free and open source, but many people have a great deal of difficulty working with it at first. The slightest error in your configuration file or the command-line startup will cause it to not run correctly.

**2) Honeypot:**

A honey pot is an interesting technology. Essentially, it assumes that an attacker can breach your network security, and it would be best to distract that attacker away from your valuable data. Therefore, a honey pot involves creating a server that has fake data perhaps an SQL server or Oracle server loaded with fake data, and just a little less secure than your real servers. Then, since none of your actual users ever access this server, monitoring software is installed to alert you when someone does access this server.

A honey pot achieves two goals. First, it takes the attacker’s attention away from the data you wish to protect. Second, it provides what appears to be interesting and valuable data, thus leading the attacker to stay connected to the fake server, giving you time to try to track the attacker.

**3) Intrusion deterrence:**

Intrusion deterrence is about making a system appear unappealing or too risky for someone to try and hack into. The idea is to make the potential reward of breaking in seem like it's not worth the effort.

One way to do this is by hiding or disguising the most valuable parts of the system, like important data or resources. This makes it harder for someone to see what they could gain from hacking in.

Another tactic is to make it seem like there's a high chance of getting caught if someone tries to break in. This can be done by putting up warnings or signs that say the system is being monitored closely.

Even if the actual security of the system hasn't changed much, just making it look less valuable or riskier can stop many potential intruders from trying. It's about creating the perception of security to discourage attacks.

**4) Intrusion Deflection:**

Intrusion deflection is becoming increasingly popular among security conscious administrators. The essence of it is quite simple: An attempt is made to attract the intruder to a subsystem set up for the purpose of observing intruders. This is done by tricking the intruder into believing that he has succeeded in accessing system resources when, in fact, he has been directed to a specially designed environment. Being able to observe the intruder while he practices his art will yield valuable clues and can lead to his arrest.

Intrusion deflection is often done by using a honey pot. Essentially, you set up a fake system, possibly a server that appears to be an entire subnet. You make that system look very attractive by perhaps making it appear to contain sensitive data, such as personnel files, or valuable data, such as account numbers or research. The actual data stored in this system is fake. The real purpose of the system is to carefully monitor the activities of any person who accesses the system. Since no legitimate user ever accesses this system, it is a given that anyone accessing it is an intruder.

**UNIT 5**

1. **Illustrate the objectives of IT act.**

The Information Technology (IT) Act, also known as the IT Act 2000, is a law in India that aims to regulate electronic commerce and prevent cybercrime. The main objectives of the IT Act can be simplified as follows:

1. **Legal Recognition of Electronic Records**: The IT Act gives legal recognition to electronic documents, digital signatures, and other electronic records. This means that electronic contracts and transactions are considered valid and enforceable in a court of law.
2. **Digital Signatures and Certificates**: The Act provides a framework for the use of digital signatures and digital certificates to authenticate electronic records and ensure their security and integrity.
3. **Regulation of Cybercrimes**: One of the key objectives of the IT Act is to combat cybercrimes such as hacking, identity theft, and data breaches. It defines various cyber offenses and prescribes penalties for committing these offenses.
4. **Data Protection and Privacy**: The Act includes provisions for the protection of sensitive personal data and information. It imposes obligations on organizations handling such data to maintain privacy and security standards.
5. **Establishment of Cyber Appellate Tribunal**: The IT Act provides for the establishment of a Cyber Appellate Tribunal to hear appeals against the orders issued by authorities under the Act.
6. **Promotion of E-Governance**: The Act aims to promote e-governance by ensuring the use of electronic means for communication, storage, and processing of government information and records.

**UNIT 6**

1. **Explain different tools used for conducting forensic analysis & examination.**

* There are a variety of tools available for conducting forensic analysis and examination. We will review a few of these. There are certainly other tools, but the ones listed here are very widely used:
* FTK: The company **AccessData** is the creator of the Forensic Toolkit, better known as simply FTK. This robust computer forensics tool allows you to recover deleted files, examine Registry settings, and perform a variety of forensic examination tasks. The software itself can be cost-prohibitive but is quite popular with law enforcement. AccessData has added additional features such as **Known File Filtering** for finding certain types of files. FTK can also search and detect files involved in child pornography. AccessData makes a phone forensics tool as well.
* EnCase: This tool, made by Guidance Software, is quite popular with law enforcement and is a direct competitor with FTK. It allows you to **image drives**, recover deleted files, examine the Registry, and carry out other common tasks. It can also be cost-prohibitive for some organizations.
* OSForensics: This is a newer tool, but one that has been well received in the forensic community. It is very low cost and easy to use. It is full featured, allowing you to recover deleted files, examine the Registry, and **search the drive**.
* Sleuth Kit: This is actually a suite of open-source tools. The full suite of tools is full featured but rather difficult to use. Each tool can require you to learn a set of command line (or shell) commands to execute.
* Oxygen: This tool is specifically for phone forensics. It does a very good job of analysing iPhones and a reasonably good job of analysing modern Android. It is not (at least currently) as effective with older Androids or Windows phones.
* Cellebrite: This is perhaps one of the most popular phone forensics tools, at least with law enforcement. It is very effective with a number of different phones. The only downside is that it is one of the most expensive phone forensics tools available.

1. **Explain the procedure for getting back deleted files.**

* It is a fact that criminals frequently attempt to destroy evidence. This is also true with computer crimes: Criminals may delete files. However, there are a variety of tools you can use to recover such files, particularly in Windows. DiskDigger is a free tool that can be used to recover Windows files. This is a very easy-to-use tool. There are more robust tools, but the fact that this is free and easy to use makes it perfect for students learning forensics. Let’s walk through its basic operation. It should be noted that all the mentioned forensics tools will recover deleted files for you. It must also be noted that there are many file recovery tools available on the Internet. DiskDigger is simply shown as an example of what is available.

On the first screen, you select the drive/partition you wish to recover files from.

On the next screen, you select the level of scan you want to do. Obviously, the deeper the scan, the longer it can take.

Then you will get a list of the files that were recovered.

You can see the file and the file header. You can also choose to recover the file if you wish. Obviously, it is possible that DiskDigger will only recover a file fragment. But that can be enough for forensics.