NETWORK SECURITY

Case Study Vocabulary 2014

**Directions**: Define each of the terms listed below.

**APTs** - An Advanced Persistent Threat is a sustained attempt to breach security by a group or organization with the resources to maintain the threat over a period.

**Bots** - Internet robots are software applications which run automated, and often repetitive, tasks over the Internet. They are used for many benign tasks such as [crawling](http://wiki.ibcsstudent.org/index.php?title=Web_crawler&action=edit&redlink=1) through large numbers of web pages in order to provide data for search engines such as Google. They can, however, be used maliciously to co-ordinate hacking attacks such as [DoS](http://wiki.ibcsstudent.org/index.php?title=Denial_of_Service_attack) attacks. When more than one bot is used for this purpose, it is referred to as a [Botnet](http://wiki.ibcsstudent.org/index.php?title=Botnet)

**Botnets** – an army of compromised machines, also known as "zombies," that are under the command and control of a single "botmaster." The rise of consumer broadband has greatly increased the power of botnets to launch crippling denial of service (DoS) attacks on servers, infect millions of computers with spyware and other malicious code, steal identity data, send out vast quantities of spam, and engage in click fraud, blackmail, and extortion. Botnets are the primary security threat on the Internet today.

**BYOD** - Bring Your Own Device is a system, often used in business or education, where individuals are permitted to bring their own computer devices and connect them to the organization's network. In this way, the user is able to access the organization's data and applications - albeit with some security implications for the company.

**DoS / DDoS attacks** - A Denial of Service attack is a malicious attack on a network system where the attackers flood a server with a large number of requests simultaneously. The aim of this is to overload the server and disrupt normal service.

**Firewalls** - A firewall is a network security device which may be made up of both hardware and software components. It is used to filter and control data passing through it in an attempt to prevent any security risks to the system it is protecting.

Firewalls use a number of different strategies for allowing or denying access. These can be based on the incoming system's [IP address](http://wiki.ibcsstudent.org/index.php?title=IP_address), domain name or port number. Firewalls can also be configured to check for hacking attacks such as [dictionary attacks](http://en.wikipedia.org/wiki/Dictionary_attack) and may deny access either for a fixed period of time or permanently. Individual IP addresses can also be added manually to a [whitelist](http://wiki.ibcsstudent.org/index.php?title=Whitelist&action=edit&redlink=1) or [blacklist](http://wiki.ibcsstudent.org/index.php?title=Blacklist&action=edit&redlink=1) which has priority and overrides the automatic settings.

**IDS** - An intrusion detection system (IDS) is a device or [software application](http://en.wikipedia.org/wiki/Software_application) that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

**IM** – Instant Messaging

**IPS** - Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are [network security](http://en.wikipedia.org/wiki/Network_security) appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.[[1]](http://en.wikipedia.org/wiki/Intrusion_prevention_system#cite_note-GIDPS-1)

**Malware** - Software that is intended to damage or disable computers and computer systems.

**Man-in-the-middle** - A Man-in-the-middle-attack describes an attack on a networked system where the attack intercepts communications between two systems and relays the messages between them. By doing this, the attacker is able to follow the conversation and may also change some of it.

**Packet-filtering** - Controlling access to a network by analyzing the incoming and outgoing [packets](http://www.webopedia.com/TERM/P/packet.html) and letting them pass or halting them based on the [IP addresses](http://www.webopedia.com/TERM/I/IP_address.html) of the source and destination.

**Proxy server** - a computer which serves as a hub through which internet requests are processed. By connecting through one of these servers, your computer sends your requests to the proxy server which then processes your request and returns what you were wanting. In this way it serves as an intermediary between your machine and the rest of the computers on the internet. Proxies are used for a number of reasons such as to filter web content, to go around restrictions such as parental blocks, to screen downloads and uploads and to provide anonymity when surfing the internet.

**Script kiddies** - are [unskilled](http://en.wikipedia.org/wiki/Unskilled) individuals who use [scripts](http://en.wikipedia.org/wiki/Scripting_language) or programs developed by others to attack computer systems and networks and [deface websites](http://en.wikipedia.org/wiki/Website_defacement). It is generally assumed that script kiddies are juveniles who lack the ability to write sophisticated hacking programs or exploits on their own, and that their objective is to try to impress their friends or gain credit in computer-enthusiast communities. The term is typically intended as an insult.

**SIEM** - **S***ecurity* **I***ncident and* **E***vent* **M***anager* is a set of tools used by [IT](http://www.webopedia.com/TERM/I/IT.html) professionals and [system administrators](http://www.webopedia.com/TERM/S/system_administrator.html) to manage multiple [security](http://www.webopedia.com/TERM/S/security.html) [applications](http://www.webopedia.com/TERM/A/application.html) and [devices](http://www.webopedia.com/TERM/D/device.html), and to respond automatically to resolve security incidents.

**Smurf attacks** - a type of denial of service attack in which a system is flooded with spoofed ping messages. This creates high computer network traffic on the victim’s network, which often renders it unresponsive.

**Spam** - refers to the use of electronic messaging systems to send out unrequested or unwanted messages in bulk.

**SSL** - a secure protocol developed for sending information securely over the Internet. SSL [encrypts](http://www.techterms.com/definition/encryption) the data being transmitted so that a third party cannot "eavesdrop" on the transmission and view the data being transmitted. Only the user's computer and the secure server are able to recognize the data.

**Stack-based buffer overflow** - an undesirable condition in which a particular computer [program](http://searchsoftwarequality.techtarget.com/definition/program) tries to use more [memory](http://searchmobilecomputing.techtarget.com/definition/memory) space than the call stack has available. In programming, the call stack is a [buffer](http://searchcio-midmarket.techtarget.com/definition/buffer) that stores requests that need to be handled. In [Windows](http://searchwindowsserver.techtarget.com/definition/Windows), a stack overflow error can be caused by certain types of [malware](http://searchmidmarketsecurity.techtarget.com/definition/malware).

**SYN flood** - a form of [denial-of-service attack](http://en.wikipedia.org/wiki/Denial-of-service_attack) in which an attacker sends a succession of [SYN](http://en.wikipedia.org/wiki/SYN_(TCP)) requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

Normally when a client attempts to start a [TCP](http://en.wikipedia.org/wiki/Transmission_Control_Protocol) connection to a server, the [client](http://en.wikipedia.org/wiki/Client_(computing)) and [server](http://en.wikipedia.org/wiki/Server_(computing)) exchange a series of messages which normally runs like this:

1. The client requests a connection by sending a SYN (synchronize) message to the server.
2. The server acknowledges this request by sending SYN-ACK back to the client.
3. The client responds with an ACK, and the connection is established.

This is called the [TCP three-way handshake](http://en.wikipedia.org/wiki/Transmission_Control_Protocol#Connection_establishment), and is the foundation for every connection established using the TCP protocol.

A SYN flood attack works by not responding to the server with the expected ACK code. The malicious client can either simply not send the expected ACK, or by [spoofing](http://en.wikipedia.org/wiki/IP_address_spoofing) the source [IP address](http://en.wikipedia.org/wiki/IP_address) in the SYN, causing the server to send the SYN-ACK to a falsified IP address - which will not send an ACK because it "knows" that it never sent a SYN.

**Threat landscape** – the areas of technology that are currently under attack by cyber criminals and hackers. Also refers to the current methods used to perform cyber-attacks.

**TLS** - a [protocol](http://searchnetworking.techtarget.com/definition/protocol) that ensures privacy between communicating [application](http://searchsoftwarequality.techtarget.com/definition/application)s and their users on the Internet. When a [server](http://whatis.techtarget.com/definition/server) and [client](http://searchenterprisedesktop.techtarget.com/definition/client) communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS supersedes and is an extension of [SSL](http://www.webopedia.com/TERM/S/SSL.html).

**Vulnerability** – An unintended flaw in [software](http://www.webopedia.com/TERM/S/software.html) code or a system that leaves it open to the potential for exploitation in the form of unauthorized access or malicious behavior such as [viruses](http://www.webopedia.com/TERM/V/virus.html), [worms](http://www.webopedia.com/TERM/W/worm.html), [Trojan horses](http://www.webopedia.com/TERM/T/Trojan_horse.html) and other forms of [malware](http://www.webopedia.com/TERM/M/malware.html).

**Whitelisting** – the use of anti-spam filtering software to allow only specified e-mail addresses to get through.

**Worm** - Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit a vulnerability on the target system or use some kind of [social engineering](http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29) to trick users into executing them. A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided.

**Zero-day attack/vulnerability** - an attack that exploits a previously unknown [vulnerability](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29) in a [computer application](http://en.wikipedia.org/wiki/Application_software), meaning that the attack occurs on "day zero" of awareness of the vulnerability.[[1]](http://en.wikipedia.org/wiki/Zero-day_attack#cite_note-1) This means that the developers have had [zero](http://en.wikipedia.org/wiki/Zero) days to address and patch the vulnerability. Zero-day [exploits](http://en.wikipedia.org/wiki/Exploit_%28computer_security%29) (the software and/or strategies that use a security hole to carry out a successful [attack](http://en.wikipedia.org/wiki/Attack_%28computing%29)) are used or shared by attackers before the developer of the target software knows about the vulnerability.

**Zombies/zombie computers** – computers under the control of a BotNet that can be used to attack sites, spread email spam, or steal important information.