**CSC 138 Final**

**Tuesday December 11 5:15-7:15PM**

**1)** **Describe the following network attacks: botnet, worm, virus, and DoS. Describe three types of DoS we reviewed. (Section 1.6)**

**Botnet-** a network of thousands of similarly compromised devices used to perform a denial of service attack

**Worm**- malware that can enter a device without any explicit user interaction. Eg:a  
user may be running a vulnerable network application to which an attacker can send malware

**Virus-** malware that require some form of user interaction to infect the user’s device

**DOS-** (Denial-of-service) DoS attack renders a network, host, or other piece of infrastructure unusable by legitimate users.

1. **Vulnerability attack.** This involves sending a few well-crafted messages to a vulnerable application or operating system running on a targeted host. If the right sequence of packets is sent to a vulnerable application or operating system, the service can stop or, worse, the host can crash.
2. **Bandwidth flooding**. The attacker sends a deluge of packets to the targeted host—so many packets that the target’s access link becomes clogged, preventing legitimate packets from reaching the server.
3. **Connection flooding.** The attacker establishes a large number of half-open or fully open TCP connections (TCP connections are discussed in Chapter 3) at the target host. The host can become so bogged down with these bogus connections that it stops accepting legitimate connections.

**2) Describe DASH and the process of video file acquisition, including the provision for clients with various bit-rates of access.**

**Dynamic Adaptive Streaming over HTTP** (DASH). In DASH, the video is encoded into several different versions, with each version having a different bit rate and, correspondingly, a different quality level. DASH allows clients with different Internet access rates to stream in video at different encoding rates. Clients with low-speed 3G connections can receive a low bit-rate (and low-quality) version, and clients with fiber connections can receive a high-quality version.

**3) Describe the DNS protocol, four services provided by DNS, the three primary levels of DNS server hierarchy, and the function of each server type.**

We need a directory service that translates hostnames to IP addresses. This is the main task of the Internet’s **domain name system (DNS).** The DNS is (1) a distributed database implemented in a hierarchy of DNS servers, and (2) an application-layer protocol that allows hosts to query the distributed database.

**4 DNS Services provided:**

1. **IP Address Translation-** The main function of DNS-- to translate hostnames to ip addresses.
2. **Host aliasing**. - DNS can be invoked by an application to obtain the canonical hostname for a supplied alias hostname as well as the IP address of the host.
3. **Mail server aliasing -** DNS can be invoked by a mail application to
4. obtain the canonical hostname for a supplied alias hostname as well as the IP address of the host.
5. **Load Distribution-** DNS is also used to perform load distribution among replicated servers, such as replicated Web servers.

**3 Levels of DNS Server Hierarchy:**

1. **Root DNS servers**. There are over 400 root name servers scattered all over the world. Root name servers provide the IP addresses of the TLD servers.
2. **Top-level domain (TLD) servers.** For each of the top-level domains — top-level domains such as .com, org, net, edu, and gov, and all of the country top-level domains such as uk, fr, ca, and jp —there is TLD server (or server cluster). TLD servers provide the IP addresses for authoritative DNS servers.
3. **Authoritative DNS servers.** An organization’s authoritative DNS server houses DNS records. An organization can choose to implement its own authoritative DNS server to hold these records; alternatively, the organization can pay to have these records stored in an authoritative DNS server of some service provider. Most universities and large companies implement and maintain their own primary and secondary (backup) authoritative DNS server.

**4. IPv4 Subnetting**

**5. Describe the process a host uses to obtain the MAC address for a host on their network given an IPv4 address**

The address resolution protocol (ARP) resolves an IP address to a MAC address. ARP resolves IP addresses only for hosts and router interfaces on the same subnet.

**6. Describe the four primary services provided by the link layer**

1. **Framing**- encapsulate network-layer datagrams within a link-layer frame before transmission over the link.
2. **Link Access-** A medium access control (MAC) protocol specifies the rules by which a frame is transmitted onto the link.
3. **Reliable Delivery-** provides link-layer reliable delivery service achieved with acknowledgments and retransmissions
4. **Error detection and correction-** provides error detection byhaving the transmitting node include error-detection bits in the frame, and having the receiving node perform an error check

**7. Define AS, BGP (and characteristics), eBGP, and iBGP.**

1. **AS-** (autonomous systems)a group of routers that are under the same administrative control
2. **BGP-** (Border Gateway Protocol) is protocol that manages how packets are routed across the internet
3. **eBGP-** a BGP connection that spans two ASs
4. **iBGP-** a BGP session between routers in the same AS

**8. Provide a brief comparison of Link State and Distance Vector algorithms.**

1. **Distance Vector Algorithms**: decentralized and does not use global information, only the cost of the links attached to its direct neighbor
2. **Link State Algorithms**: a centralized algorithm b/c it requires each node to first obtain a complete map of the network before running the Dijkstra algorithm.

**9. Provide a definition and function/purpose for the following: RFC, IETF, IEEE, IANA, and VLAN**

1. **RFC-** (Request for comments)the name for IETF’s standards documents
2. **IETF-** stands for Internet Engineering Task Force who develop the internet standards
3. **IEEE**- (Institute of Electrical and Electronics Engineers) - creates networking standards
4. **IANA-** (Internet Assigned Numbers Authority): its function is the global coordination of the Internet Protocol addressing systems (IP addresses)
5. **VLAN**- virtual local area networks can be defined over a single physical local area network infrastructure.