**CSC 138 Final Exam Study Guide**

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

- Botnet: Network of compromised devices controlled by malicious users

- Worm: Self-replicating malware that doesn’t require user interaction to infect a device

- Virus: Self-replicating malware that requires user interaction to infect a device

- DoS (Denial-of-Service): Renders a piece of infrastructure unusable by legitimate users

- Vulnerability Attack: Attacker exploits vulnerabilities on an application or operating system by sending well-crafted messages, stopping the service or crashing the host

- Bandwidth Flooding: Attacker sends flood of packets to target host, clogging the access link and preventing legitimate packets from reaching server

- Connection Flooding: Attacker establishes many TCP connections at target host, so 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

- Server:

- Divides video file into multiple pieces

- Pieces stored and encoded at different rates

- Manifest file provides URLs for different pieces

- Client:

- Periodically measures server-to-client bandwidth

- Consulting manifest file, requests one piece at a time

- Can choose different coding rates at different points in time, depending on currently available bandwidth

*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.*

- Domain Name System

- DNS Protocol: Application layer, UDP, allows hosts to query the distributed database used in DNS

- Four Services:

- Hostname to IP address translation, host aliasing, mail server aliasing, load distribution

- Hostname to IP address translation: Translates mnemonic hostname (e.g. www.example.com) to a corresponding router usable IP address

- Host Aliasing: Associates complicated canonical hostnames with more mnemonic alias hostnames

- Mail Server Aliasing: Associates complicated canonical mail server hostnames with more mnemonic alias hostnames

- Load distribution: Rotates order of replicated server IP addresses given in query responses, distributing traffic among the replicated servers

- Three Levels:

- Root DNS servers, TLD (Top-Level Domain) servers, authoritative DNS servers

- Root DNS Servers: Provides IP addresses of TLD servers

- TLD Servers: Provides IP addresses of authoritative DNS servers

- Authoritative DNS Servers: Provides IP addresses of an organization’s publicly accessible hosts

*4. IPv4 addressing / subnetting*

- Do related exercises

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

- MAC: Media Access Control

- ARP (Address Resolution Protocol) used to translate between IP and MAC addresses for hosts and routers on same LAN (local area network)

- Each node on network keeps ARP table, used to hold IP/MAC address mappings

- Sender broadcasts ARP query packet containing receiver’s IP addresses

- Receiver receives ARP query packet, replies with its MAC addresses

- Sender saves IP/MAC address mapping in ARP table until times out

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

- Framing, link access, reliable delivery, error detection and correction

- Framing: Encapsulates network-layer datagram within data field of link-layer frame before transmission

- Link Access: MAC protocol coordinates frame transmissions when multiple nodes share single link, specifies rules for frame transmissions

- Reliable Delivery: Guarantees datagram is moved across link without error

- Error Detection and Correction: Transmitting node includes error detection bits, receiving node performs error check

- Tries to correct error locally instead of forcing re-transmission

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

- AS (Autonomous System): group of routers under the same administrative control

- BGP (Border Gateway Protocol): Inter-AS routing protocol that all AS’s run

- Routing information exchanged over TCP connections

- Distance vector algorithm, too many routers to know for link state

- eBGP (External BGP): BGP connection between two AS’s

- iBGP (Internal BGP): BGP connection between routers in the same AS

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

- Link State: All routers have identical and complete view of network-layer

- Routers compute same set of least-cost paths as every other router

- Each node computes only its own table

- Distance Vector: Router knows physically connected neighbors and link costs to neighbors

- Iterative process, exchange of information with neighbors

- Each node’s table used by others

*9. Provide a definition and function/purpose for the following: RFC, IETF, IEEE, IANA, and VLAN (802.1q).*

- RFC (Request for Comments): Formal document drafted by the IETF describing the specifications for a particular technology

- IETF (Internet Engineering Task Force): Organization that develops Internet standards

- IEEE (Institute of Electrical and Electronics Engineers): Organization of technical professionals working for the advancement of electrical technology

- IANA (Internet Assigned Numbers Authority): Organization tasked with overseeing the allocation of IP addresses

- VLAN (Virtual Local Area Network): Group of hosts that behave as if they are connected to the same broadcast domain regardless of physical location

- Provides traffic isolation, efficient use of switches, and user management

- 802.1q (Trunking): Carries frames between VLANs defined over multiple physical switches